Deutscher Bundestag
8. Wahlperiode

Drucksache 8/2460

10. 01. 79

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)

Gliederung

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, Herderstraße 56, 5300 Bonn 2, Telefon (0 22 21) 36 35 51

Gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 008/1 — vom 10. Januar 1979.

1 Die Aufgaben des Bundesbeauftragten und ihre organisatorische Durchführung

1.1 Zweckbestimmung und gesetzliche Grundlagen der Einrichtung des Bundesbeauftragten für den Datenschutz

Der Gedanke, den Rechtsschutz des einzelnen bei der Datenverarbeitung durch eine besondere staatliche Kontrollinstanz zu gewährleisten, wurde im Parlament geboren. Der Regierungsentwurf eines Bundesdatenschutzgesetzes (BDSG) (BT-Drucksache 7/1027) sah eine solche Einrichtung noch nicht vor; erst in den Ausschußberatungen des Gesetzentwurfes nahm die Idee Konturen an, zusätzlich zu den eigenen Kontrollmechanismen der öffentlichen Verwaltung eine Fremdkontrolle zu fordern und sie einer besonderen, unabhängigen Institution anzuvertrauen. Unterstützt wurden diese Überlegungen durch die Äußerungen zahlreicher Wissenschaftler, Verbände und sonstiger kompetenter Stellen in den von der Bundesregierung und vom Deutschen Bundestag veranstalteten Anhörungen zum Entwurf eines BDSG. Dabei konnte auf die guten Erfahrungen hingewiesen werden, welche die Länder Hessen und Rheinland-Pfalz mit ihren Datenschutzinstanzen gemacht haben.

Die gesetzliche Grundlage für die Einrichtung des Bundesbeauftragten ist in den §§ 17 und 18 BDSG enthalten, die zusammen mit den Vorschriften über die Bestellung von Datenschutzbeauftragten bei nicht-öffentlichen Stellen bereits am 1. Juli 1977 in Kraft traten.

1.2 Rechtsstellung des Bundesbeauftragten

Der Bundesbeauftragte für den Datenschutz steht zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Seine Amtszeit beträgt fünf Jahre; die einmalige Wiederbestellung ist zulässig. Der Bundesbeauftragte ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des Bundesministers des Innern.

Auf Vorschlag der Bundesregierung hat mich der Bundespräsident mit Urkunde vom 13. Februar 1978 zum ersten Bundesbeauftragten für den Datenschutz ernannt; die Urkunde wurde mir am 14. Februar 1978 vom damaligen Bundesminister des Innern, Professor Dr. Werner Maihofer, ausgehändigt.

1.3 Die Einrichtung der Dienststelle

1.3.1 Zuordnung zum Bundesministerium des Innern

Die Dienststelle des Bundesbeauftragten ist nach § 17 Abs. 5 BDSG beim Bundesminister des Innern eingerichtet worden; ihre Personal- und Sachausgaben sind in einem eigenen Kapitel des Einzelplans 06 des Bundeshaushalts ausgewiesen.

Alsbald nach Inkrafttreten der §§ 17, 18 BDSG wurde als Kern der neuen Dienststelle ein Aufbaustab eingesetzt, der die Voraussetzungen für die Erfüllung der Sachaufgaben zu schaffen und die notwendigen Kontakte zu knüpfen hatte, zugleich aber auch schon im Vorgriff auf das ab 1. Januar 1978 geltende materielle Datenschutzrecht erste Aktivitäten entwickelte. Um dem zu jener Zeit noch nicht bestimmten Amtsinhaber nicht vorzugreifen, besetzte der Bundesminister des Innern nicht alle im Haushaltsjahr 1977 zur Verfügung stehenden Stellen. In der Folgezeit ist der Minister seiner gesetzlichen Verpflichtung, mir die für die Erfüllung meiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen, in hervorragender Weise nachgekommen.

1.3.2 Personal

Bereits im Herbst 1976 hatte der Bundesminister des Innern eine Personalbedarfsplanung für die Dienststelle des Bundesbeauftragten aufgestellt und mit dem Bundesminister der Finanzen abgestimmt. Danach wurde — vorbehaltlich praktischer Erfahrungen — ein personeller Endausbau der Dienststelle mit insgesamt 36 Mitarbeitern einschließlich der Hilfskräfte als Minimalausstattung ermittelt und vorgesehen, daß die entsprechenden neuen Stellen in mehreren Jahresraten beantragt werden sollten. Nachdem außer der Stelle des Bundesbeauftragten in den Jahren 1977 elf Stellen und 1978 acht Stellen bewilligt und besetzt wurden, sind im Entwurf des Bundeshaushalts 1979 weitere elf Stellen veranschlagt worden. Es ist zu hoffen, daß der endgültige Personalstand im Jahre 1980 erreicht werden kann.
Die derzeit vorhandenen Stellen setzen sich wie folgt zusammen: höherer Dienst: 8, gehobener Dienst: 3, mittlerer Dienst: 2, Tarifangestellte: 5 Stellen, Arbeiter: 1 Stelle.

Da die sachliche Unabhängigkeit der Absicherung durch eine personelle Entscheidungskompetenz bedarf, habe ich mir vom Bundesminister des Innern im Rahmen der dienstrechtlichen Bestimmungen ein weitgehendes Mitwirkungsrecht bei der Stellenbesetzung ausbedungen. Meinen Vorschlägen zur Besetzung der aus dem Jahre 1977 noch offenen und der im Jahre 1978 neu zugewiesenen Stellen wurde ausnahmslos entsprochen.

Die Personalauswahl, die zum Teil aufgrund einer Stellenausschreibung vorgenommen wurde, erwies sich als schwierig, weil die Aufgabe einerseits Kenntnisse der Datenverarbeitung, andererseits aber auch die Kenntnis der Organisation und der Arbeits-

abläufe der Bundesverwaltung voraussetzt. In Fachkreisen, insbesondere in der Privatwirtschaft, wo in großer Zahl betriebliche Datenschutzbeauftragte mit ähnlichem Anforderungsprofil bestellt werden müssen, wird diese Problematik lebhaft diskutiert.

Ich habe mich bemüht, ein ausgewogenes Verhältnis zwischen Datenverarbeitungs- bzw. Datenschutzkenntnissen und Verwaltungserfahrung herzustellen. Besonderes Gewicht hatte das Auswahlkriterium des Engagements für den Datenschutz; daneben waren für die verschiedenen Teilbereiche Spezialkenntnisse bestimmter Verwaltungs- oder Sachbereiche erforderlich. Die Tätigkeit des Bundesbeauftragten für den Datenschutz besteht nach den bisherigen Erfahrungen vorwiegend in der Rechtsanwendung und -entwicklung; sie hat auch dort in erheblichem Maße Bezug zu Rechtsfragen, wo es um die Kontrolle der Datenverarbeitung „vor Ort" geht. Dementsprechend habe ich die Stellen des höheren Dienstes zum größten Teil mit Juristen besetzt, vorzugsweise mit solchen, die einschlägige Erfahrungen mit der Datenverarbeitung aufweisen konnten, daneben konnte aber auch Sachverstand auf anderen Gebieten (Mathematik, Informatik, Wirtschaftswissenschaft) einbezogen werden. Auch im gehobenen Dienst sind Erfahrungen und Fachkenntnisse aus der praktischen Datenverarbeitung vorhanden.

Die Mitarbeiter des höheren und gehobenen Dienstes stammen je zur Hälfte aus dem Bereich des Bundesministeriums des Innern und aus anderen Bereichen (Wissenschaft und Forschung, andere Verwaltungen). Sämtliche Mitarbeiter gehören dienstrechtlich zum Bundesministerium des Innern und werden durch dessen Personalrat mitvertreten. Dadurch ist die Möglichkeit des Personalaustausches mit dem großen Personalbestand des Bundesministeriums gewährleistet.

1.3.3 Organisation der Dienststelle

Die Zuständigkeiten konnten in der Aufbauphase nur vorläufig verteilt werden. Nach den inzwischen vorliegenden Erfahrungen wurde eine Gliederung in die folgenden Referate vorgenommen:

In einem Grundsatzreferat, das von dem Leitenden Beamten der Dienststelle wahrgenommen wird, werden rechtliche und technische Grundsatzfragen des Datenschutzes einschließlich der Kooperation mit den Datenschutzbeauftragten der Länder bearbeitet. Hier soll auch das Dateienregister geführt werden; angegliedert sind die zentralen Dienste (Registratur, Hausverwaltung, Bibliothek). Vier weitere Referate betreuen die Datenschutzkontrolle in größeren Aufgabenbereichen der Bundesverwaltung, für deren Zusammenfassung teils Sachaspekte, teils besondere Kenntnisse und Erfahrungen der Referatsangehörigen maßgebend waren. So hat sich die Zusammenfassung der folgenden Gebiete in jeweils einem Referat als zweckmäßig erwiesen:

— Innere Verwaltung, Rechtswesen, Finanzen, Internationales

— Soziale Sicherung, Gesundheitswesen, Personalwesen, Öffentlichkeitsarbeit

— Wirtschaft, Verkehr, Statistik, Wissenschaft, Medien, nicht-öffentlicher Bereich

— Öffentliche Sicherheit, Verteidigung.

Die breite Ausfächerung der Zuständigkeiten in den Ressorts der Bundesverwaltung macht auch in der Dienststelle des Bundesbeauftragten eine gewisse Spezialisierung der Mitarbeiter notwendig. Die referatsübergreifende Aufgabe der Kontrollen „vor Ort" konnte bisher erst von einem Referat (Soziale Sicherung usw.) aufgenommen werden; sie wird künftig von einer Prüfgruppe wahrgenommen werden, die unter der Leitung eines mathematisch-betriebswirtschaftlich vorgebildeten Mitarbeiters beim Grundsatzreferat angesiedelt wird und die dann noch besser in der Lage sein wird, die Referate in technisch-organisatorischen Angelegenheiten und in Fragen der Datensicherung zu unterstützen.

Die Referate sind teilweise personell noch unzureichend ausgestattet; so ist das praktisch sehr wichtige Referat, das sich mit der Datenverarbeitung im Bereich der Sicherheitsbehörden befaßt, mangels Stellen bisher noch ohne „Unterbau". Das Referat mit dem größten Arbeitsanfall (Wirtschaft, Verkehr usw.), das insbesondere die Zusammenarbeit mit den Datenschutzinstanzen für den nicht-öffentlichen Bereich zu pflegen hat, bedarf ebenfalls der Verstärkung. Ich hoffe sehr, daß diese Mängel durch weitere Stellenzuweisungen behoben werden können.

1.3.4 Räumlichkeiten

Der personelle Aufbau der Dienststelle — der sich über das ganze Berichtsjahr hinzog — führte dazu, daß eine Unterbringung der Mitarbeiter im Gebäudekomplex des Bundesministeriums des Innern nicht mehr möglich war. Für meine Dienststelle wurde deshalb ein eigenes Dienstgebäude in Bonn-Bad Godesberg, Stephan-Lochner-Str. 2, angemietet. Die räumliche Abtrennung vom Bundesministerium des Innern betont zugleich die fachliche Unabhängigkeit. Das im September 1978 bezogene Gebäude ist funktionell hervorragend geeignet. Auch bei der Beschaffung dieser Räume und ihrer Ausstattung hat mich der Bundesminister des Innern in dankenswerter Weise unterstützt.

1.4 Die Bedeutung der verschiedenen Aufgaben

1.4.1 Die Kontrollaufgabe

In der Bestimmung über den Aufgabenkreis des Bundesbeauftragten (§ 19 BDSG) ist die Kontrollaufgabe an den Anfang gestellt. Der Bundesbeauftragte für den Datenschutz (BfD) hat die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen der Bundesverwaltung — bei den Gerichten nur, soweit sie in Verwaltungsangelegenheiten tätig werden — einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zu überwachen. Es liegt auf der Hand, daß dies eine Aufgabe von

großem Umfang und ausgeprägter Heterogenität darstellt; die Kontrollinstanz muß sich mit den fachlichen und verfahrensmäßigen Besonderheiten einer Vielzahl von Stellen der Bundesverwaltung vertraut machen, deren Aufgaben, soweit sie für mich von Interesse sind, von der Verwaltung von Archivgut bis zur Beobachtung von Spionageversuchen reichen. Die Kontrolle muß sich sowohl auf die Einhaltung der materiellen Bestimmungen des Datenschutzrechts erstrecken — wobei insbesondere die Frage der Erforderlichkeit der Datenverarbeitung zu dem jeweiligen Verwaltungszweck intensive Überlegungen nötig macht — als auch die Datensicherheit gewährleisten, was zu Untersuchungen über mögliche Fehler bis hin zu kriminellen Vergehen führt und in großem Maße technisch-organisatorische Analysen erfordert.

Da das Personal der Dienststelle im Berichtsjahr erst angeworben werden mußte und es vielen der ausgewählten Mitarbeiter nicht möglich war, ohne Übergangsfrist die neue Tätigkeit aufzunehmen, konnten größere Kontrollen bei Bundesbehörden erst in einigen Fällen stattfinden (vgl. 3.5.3). Doch wurden die Voraussetzungen für die Kontrolltätigkeit auch in weiteren Bereichen der Bundesverwaltung dadurch geschaffen, daß ich mich mit den zuständigen Mitarbeitern zu den betreffenden Stellen begeben habe, wo wir uns über die grundlegenden Organisationsfragen informieren ließen. Aufgrund von Einzeleingaben von Bürgern oder auf Anstoß der Medien wurden außerdem Prüfungen vorgenommen, die die Rechtmäßigkeit der Datenverarbeitung in bezug auf bestimmte Betroffene zum Gegenstand hatten. Mit dem weiteren Ausbau der Dienststelle wird es möglich sein, in zunehmendem Maße auch systematische Kontrollen durchzuführen.

1.4.2 Die Beratungs- und Entwicklungsaufgabe

Die Beratung der Bundesbehörden in Fragen des Datenschutzes (vgl. § 19 Abs. 1 Satz 2 BDSG) ist aus meiner Sicht fast noch wichtiger als die nachgehende Kontrolle — so bedeutsam diese in manchen Fällen wegen ihrer Signalwirkung sein kann. Die präventive Beratung der öffentlichen Stellen des Bundes kann dazu beitragen, daß es gar nicht erst zu Verstößen kommt.

Ich habe deshalb unmittelbar nach meinem Amtsantritt an alle Bundesminister geschrieben und ihnen meine Unterstützung und Beratung in Datenschutzfragen angeboten; die Reaktion war durchweg positiv und führte in der Folgezeit zu zahlreichen persönlichen Kontakten und Gesprächen mit den zuständigen Stellen, insbesondere mit den für den Datenschutz verantwortlichen Beamten der Ressorts.

Die vom Gesetz mir eingeräumte Möglichkeit, Empfehlungen zur Verbesserung des Datenschutzes zu geben, begreife ich im rechtspolitischen Sinne, nämlich so, daß von mir — aus meiner Kontrollerfahrung und den dabei gewonnenen Erkenntnissen über Schwachstellen der Gesetzeslage heraus — auch Vorschläge zur Verbesserung des Datenschutzrechts erwartet werden. Diese Interpretation wird einmal durch die bereits im Gesetzgebungsverfahren zum BDSG wiederholt getroffene Feststellung gestützt, daß das BDSG als eine völlig neue Rechtsmaterie ohne vergleichbares Vorbild in anderen Rechtsordnungen in seiner Anwendung besonders kritisch unter dem Gesichtspunkt betrachtet werden müsse, ob Novellierungen nötig sind, daß das Gesetz zum anderen aber wegen seiner umfassenden Geltung zahlreiche Generalklauseln verwenden mußte, für deren Konkretisierung erst die praktische Anwendung Hinweise geben kann, die sich möglicherweise in Rechtsnormen umsetzen lassen. Erste Überlegungen zur Verbesserung des Gesetzes enthält bereits dieser Tätigkeitsbericht (vgl. Abschnitt 4). Viele Fragen sind aber gegenwärtig noch nicht entscheidungsreif, weil noch Erfahrungen über die Anwendung fehlen, zum Teil auch nicht formulierungsreif, weil unterhalb der Ebene des Gesetzes eine Vielzahl von Richtlinien und Klauseln (Einwilligungserklärungen u. ä.) erprobt werden, deren Wirkungen noch nicht verglichen werden konnten. Konkrete Änderungsvorschläge werde ich in meinen künftigen Tätigkeitsberichten vorlegen. Die Forderung nach Novellierung des BDSG verliert auch in dem Maße an Dringlichkeit, wie bereichsspezifische gesetzliche Regelungen zustande kommen. Gegenwärtig besteht zumindest in zwei wichtigen Bereichen Aussicht auf eine solche gesetzliche Neuregelung, nämlich für die Datenverarbeitung im Bereich der Sozialen Sicherung und darüber hinaus — mit Auswirkungen für einen wichtigen Verwaltungsbereich der Länder — für das Meldewesen (dazu unten 3.2.2).

In den Zusammenhang der Beratungsaufgabe gehört auch die gesetzliche Verpflichtung des Bundesbeauftragten, auf Anforderung des Deutschen Bundestages oder der Bundesregierung Gutachten zu erstellen und Berichte zu erstatten (§ 19 Abs. 2 Satz 1 BDSG). Auf die bisherigen Aktivitäten in dieser Richtung wird weiter unten näher eingegangen werden (3.2.2, s. a. — Stellungnahme gegenüber dem Bundesverfassungsgericht — 3.4.7.4). Dem Innenausschuß des Deutschen Bundestages habe ich einen ersten mündlichen Bericht über meine Tätigkeit in seiner Sitzung am 18. Oktober 1978 erstattet.

1.4.3 Die Ombudsman-Aufgabe

Nach § 21 BDSG kann sich jedermann an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Behörden der Bundesverwaltung in seinen Rechten verletzt worden zu sein. Der Bundesbeauftragte ist hiernach eine Art Ombudsman, „Bürgeranwalt" in Datenschutzfragen.

Tatsächlich ist eine Fülle von Anfragen, Eingaben und Auskunftsersuchen an mich gelangt. In mehr als tausend Fällen konnte ich entweder selbst helfen oder das vorgetragene Anliegen an die zuständigen Stellen weiterleiten.

Es ist aufschlußreich, welche Probleme von den Bürgern in ihren Briefen an den Bundesbeauftragten aufgeworfen worden sind. Deshalb seien hier einige besonders häufig vorkommende Fragen wiedergegeben:

— Viele Bürger sind durch unverlangte Werbezusendungen beunruhigt, weil sie vermuten, daß sie aufgrund bestimmter Angaben in den Empfängerkreis einbezogen wurden, jedoch nicht erkennen können, um welche es sich dabei handelt und von welcher Stelle die Daten zur Verfügung gestellt wurden. In diesen Zusammenhang gehört auch die Kritik an der Praxis einiger Behörden, Anschriften, die für Zwecke des Verwaltungsvollzugs gesammelt wurden, für Zwecke von Meinungsforschung und Werbung zu veräußern.

— Von vielen wird als ungerecht empfunden, daß für eine Auskunft über die eigenen Daten ein Entgelt bzw. eine Gebühr verlangt wird, zumal dann, wenn die Betroffenen die Speicherung gar nicht veranlaßt haben (wie bei Auskunfteien und anderen Informationsstellen des Kreditgewerbes). Auch die Höhe des Entgelts wird häufig als unangemessen angesehen.

— Die Klauseln, mit denen zum Beispiel Versicherungen eine Einwilligung zur Datenübermittlung einholen, sind für die Bürger unverständlich. Man fürchtet, der speichernden Stelle eine Blankovollmacht zur beliebigen Verfügung über die personenbezogenen Daten zu erteilen.

— Bei — privaten wie amtlichen — Erhebungen wird Kritik daran geübt, daß die Fragen oft tief in den Bereich des einzelnen vorstoßen. Jedenfalls dann, wenn der Betroffene aus den Unterlagen bestimmbar ist, wird dies als unzumutbarer Eingriff angesehen. Überdies wird häufig in Zweifel gezogen, ob die erhobenen Daten vor dem Zugriff Unbefugter tatsächlich gesichert sind.

— Ein häufig vorgebrachtes Anliegen betrifft das Verhältnis von Ärzten, Krankenhäusern und Patienten. So wird die Verletzung von Auskunftsrechten der Patienten behauptet. In vielen Eingaben kommt die Angst vor dem Mißbrauch ärztlicher, insbesondere psychiatrischer Gutachten für Zwecke der Personal- und Arbeitsverwaltungen zum Ausdruck. Schließlich teilten Ärzte ihre Bedenken gegen neuere gesetzliche Regelungen mit, die auf eine Durchbrechung des Arztgeheimnisses durch die Verwaltung hinausliefen.

— Eine relativ erhebliche Zahl von Eingaben beruht darauf, daß Bürger sich durch bestimmte vermutete Maßnahmen des Bundeskriminalamts und/oder der Nachrichtendienste sowie der Wehrersatzbehörden beeinträchtigt fühlen (über Art und Ergebnisse der bisher durchgeführten Einzelprüfungen vgl. 3.4.3 bis 3.4.5). Hinzu kommt eine Reihe von Eingaben, in denen ohne konkreten Anlaß generell Befürchtungen gegenüber der Tätigkeit der Sicherheitsbehörden geäußert werden.

Nicht immer konnte die Antwort für die Betroffenen befriedigend ausfallen. Zu einem nicht unbeträchtlichen Teil muß ich an andere Stellen, nämlich die Aufsichtsbehörden für den Datenschutz in den Ländern und — soweit schon eingerichtet — die Landesdatenschutzbeauftragten verweisen. Die Zuständigkeitsverteilung im Bundesstaat ist kompliziert, die Kompetenzregelungen bringen zusätzliche Differenzierungen — so war es nicht verwunderlich, daß viele Bürger sich an denjenigen wandten, dessen Name und Funktion einer größeren Öffentlichkeit schon bekannter war, also an den Bundesbeauftragten für den Datenschutz, auch wenn es um Angelegenheiten ging, die die Datenverarbeitung bei nichtöffentlichen Stellen oder in Landesverwaltungen betrafen. Wenn ein Kommentator des Bundesdatenschutzgesetzes den Bundesbeauftragten als „Gewissen des Datenschutzes" bezeichnet, so entspricht dies nach meinen Erfahrungen den Erwartungen eines breiten Publikums. Wo ich diesen Erwartungen mangels Zuständigkeit zu Aufsichtsmaßnahmen nicht gerecht werden konnte, habe ich doch an der öffentlichen Diskussion über die angesprochenen Fragen und an den Koordinationsbestrebungen der Landesbehörden teilgenommen (vgl. § 19 Abs. 5 BDSG) und teilweise rechtspolitische Vorschläge gemacht. Auch die Eingaben, deren Bearbeitung ich anderen Stellen überlassen muß, vermitteln mir Erkenntnisse darüber, welche Datenschutzprobleme aus der Sicht der Bürger bestehen und ob sie mit dem geltenden Datenschutzrecht gelöst werden können.

1.4.4 Kooperation mit anderen Datenschutzinstanzen

Zur Erfüllung der soeben angesprochenen Kooperationsaufgabe habe ich im Berichtsjahr zweimal die Vertreter der für den nicht-öffentlichen Bereich zuständigen obersten Landesaufsichtsbehörden und die bereits eingesetzten Landesbeauftragten für den Datenschutz eingeladen. In diesem Rahmen konnten in nützlicher Weise Informationen ausgetauscht und Grundsatzfragen des Datenschutzes besprochen werden. Ferner beteilige ich mich an dem regelmäßig stattfindenden Erfahrungsaustausch der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich, wo insbesondere zu problematischen Einzelfällen Stellung genommen und eine Abstimmung des Vorgehens angestrebt wird. Gegen Ende des Jahres hat sich ferner auf Initiative des Hessischen Datenschutzbeauftragten eine Konferenz der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz konstituiert, die ebenfalls der Abstimmung der Datenschutzpraxis dient. Gute Kontakte bestehen auch mit dem Petitionsausschuß und dem Wehrbeauftragten des Deutschen Bundestages.

Ich halte diese Formen der Zusammenarbeit — jede auf ihre Weise — für notwendig, aber auch für ausreichend, um dem gesetzlichen Auftrag gerecht zu werden und zu einer einheitlichen Handhabung des Datenschutzrechts zu gelangen.

1.4.5 Dateienregister

Nach § 19 Abs. 4 BDSG führt der Bundesbeauftragte ein Register der automatisch betriebenen Dateien, in denen personenbezogene Daten gespeichert werden. Dieses Register hat dieselbe Publikationsfunktion, wie die Pflicht der Behörden nach § 12 Abs. 1 BDSG, bestimmte Angaben über die von ihnen geführten Dateien zu veröffentlichen. Die ersten Anmeldungen zu diesem Register gingen bereits im Juli 1978 bei mir ein. Die übersandten Beschreibungen waren allerdings so unterschiedlich, daß sie

für den Bürger kaum verständlich und als Hilfsmittel für meine Kontrolltätigkeit wenig brauchbar gewesen wären. Einige Meldungen waren auch ungenau.

Damit das Register seine vorgesehenen Funktionen voll erfüllen kann, habe ich Hinweise für die Meldungen herausgegeben, die die Datenschutzregisterordnung erläutern und für Verständlichkeit und eine gewisse Einheitlichkeit der Meldungen sorgen sollen. Außerdem wurden viele Stellen bei der Formulierung einzelner Meldungen unterstützt.

Bis zum 31. Dezember 1978 hatten 72 öffentliche Stellen des Bundes insgesamt 476 automatisch betriebene Dateien, in denen personenbezogene Daten gespeichert werden, zum Dateienregister angemeldet. Gleichartige Stellen mit lediglich unterschiedlichen örtlichen Zuständigkeitsbereichen (z. B. bei der Bundespost) wurden dabei jeweils als nur eine Stelle gezählt. Eine Reihe von Meldungen steht noch aus.

Die eingegangenen Meldungen betreffen

163 Dateien über dienst- und arbeitsrechtliche Verhältnisse der Beschäftigten dieser Stellen,

126 Dateien über Wirtschaftsbeziehungen zu Lieferanten oder Kunden,

16 andere Dateien, die ausschließlich oder überwiegend dem Zahlungsverkehr zwischen den Stellen und den Betroffenen dienen,

20 Adreßdateien (Verteiler) für die regelmäßige Versendung von Veröffentlichungen, Rundschreiben u. ä.,

10 Bibliothekskataloge und andere Nachweissysteme für überwiegend fachspezifische Literatur,

36 Dateien für Aufgaben der Förderung, Durchführung und Koordination der fachspezifischen Forschung und

105 Dateien für sonstige Zwecke, z. B. Einfuhrgenehmigungen für bestimmte Waren usw.

Außerdem haben die Ersatzkassen und die Betriebskrankenkassen durch ihre Verbände die Dateien über ihre Versicherten, die zahlungspflichtigen Arbeitgeber und die Vertragspartner und Lieferanten sowie die Adreßdateien für die Verteilung ihrer Publikationen angemeldet.

Das Register kann nach § 19 Abs. 4 Satz 2 BDSG von jedem eingesehen werden. Ich erwäge, das Register — etwa nach dem Vorbild des Auskunftssystems, das der Ausschuß für Datenschutz beim Landtag von Rheinland-Pfalz aufgebaut hat — automatisch zu betreiben. Doch kann eine Entscheidung über die Frage, ob diese Form zweckmäßig und wirtschaftlich ist, erst getroffen werden, wenn die Meldungen vollständig vorliegen und erste Erfahrungen mit der Benutzung des Registers gemacht sind. Zur Kritik an der gesetzlichen Regelung des Dateienregisters siehe unten 4.5.3.

2 Schwerpunkte der Tätigkeit im Berichtsjahr

2.1 Beobachtung der Entwicklungen und Information der Öffentlichkeit

Die Institution eines Bundesbeauftragten für den Datenschutz hat, wie bereits ausgeführt (1.1), Vorläufer in der des Hessischen Datenschutzbeauftragten und des Ausschusses für Datenschutz beim Landtag Rheinland-Pfalz. Erfahrungen dieser Stellen konnten ausgewertet werden, aber die Situation auf Bundesebene und nach Erlaß eines umfassenden Bundesdatenschutzgesetzes stellte sich in wesentlichen Punkten anders dar als in den genannten beiden Ländern.

Die neue Behörde mußte sogleich auf eine Vielzahl von Anforderungen und Erwartungen reagieren und gleichzeitig ein Arbeitsprogramm entwickeln, um die Verwirklichung des gesetzlichen Auftrages so schnell wie möglich beginnen zu können. Das bedeutete, daß die Entwicklungen in der Datenverarbeitung — und zwar in Staat *und* Wirtschaft — beobachtet und in wichtigen Bereichen vertieft erkundet werden mußten; gleichzeitig war eine umfangreiche Informationsarbeit gegenüber der Öffentlichkeit zu leisten. Ich bin vom ersten Tage meiner Amtszeit an von zahllosen Bürgern und ihren Repräsentanten in den Medien und anderen Organisationen um Informationen gebeten worden. Das Bedürfnis, die Rechte des Bürgers nach dem neuen Gesetz kennenzulernen, war ungewöhnlich groß. Die Medien tragen in verdienstvoller Weise dazu bei, Kenntnisse der neuen Materie zu verbreiten. Ich selbst habe eine Informationsschrift mit leicht verständlichen Erläuterungen des schwierigen Rechtsgebiets herausgegeben. Täglich erhalte ich eine Fülle von Nachfragen nach dieser Schrift, die inzwischen eine Auflage von rd. 54 000 Exemplaren hat und nahezu vergriffen ist.

Zu meinem Bedauern kann ich wegen der knapp bemessenen Haushaltsmittel nicht alle Informationswünsche befriedigen.

Es wird mehrjähriger Anstrengungen und vielfältiger Formen bedürfen, um eine allgemeine Kenntnis der Bürgerrechte zum Datenschutz zu erreichen. Das Bewußtsein für die Notwendigkeit von Datenschutz ist — entgegen manchen skeptischen Bemerkungen — durchaus im Wachsen, aber es fehlt weithin noch an Informationen sowohl über den tatsächlichen Umfang und die Art und Weise von Datenverarbeitung wie über die rechtlichen Regelungen. So erhalte ich nach wie vor immer wieder Auskunftsersuchen von Bürgern, die davon ausgehen, daß ihre personenbezogenen Daten bei meiner Dienststelle gespeichert seien. Daß dies nicht der Fall ist, läßt sich leicht erklären, aber die häufig er-

betene Auskunft, wo denn die Daten einer Person gespeichert seien, kann detailliert und exakt überhaupt nicht, in Umrissen und mit einer gewissen Wahrscheinlichkeit allenfalls nur in Ausnahmefällen erteilt werden. Ich beabsichtige, im Laufe des Jahres 1979 eine Broschüre herauszugeben, die dazu beiträgt, den tatsächlichen Stand der Datenverarbeitung in der Bundesverwaltung und in anderen Bereichen anschaulich zu machen und dadurch dazu beizutragen, daß der Bürger sich in diesem Feld besser orientieren kann.

2.2 Inhaltliche Schwerpunkte der Tätigkeit

Alle Anfragen und Informationsbitten von Bürgern, die sich an mich gewandt haben, sind beantwortet worden; zu allen oben aufgeführten Themenkreisen (1.4.3) sind zumindest erste Überlegungen angestellt worden und Gespräche mit vielen beteiligten Stellen aufgenommen worden. Einige Problembereiche haben sich aber als Schwerpunkte herausgestellt.

Es waren dies:

— Die Auswirkungen des Datenschutzrechts bei den Sicherheitsbehörden (dazu im einzelnen 3.4),

— die datenschutzrechtlichen Probleme der Sozialversicherungsträger, insbesondere das Sozialgeheimnis und seine Neuregelung (dazu 3.5),

— die Gesetzgebung zum Meldewesen (3.2.2) und

— die Beobachtung der Auswirkungen des Bundesdatenschutzgesetzes in bestimmten Bereichen der Wirtschaft (Kreditschutz, Versicherungswirtschaft) (dazu 3.7).

Diese Schwerpunktbildung ist teilweise mitverursacht durch die politische Entwicklung und öffentliche Diskussionen im Laufe des Berichtsjahres, sie spiegelt andererseits auch wider, welche Gefahren für Bürgerrechte in der Öffentlichkeit als besonders bedrohlich angesehen werden.

2.3 Wichtige Erkenntnisse der bisherigen Amtstätigkeit

Bevor ich auf den Stand des Datenschutzes in einzelnen Bereichen eingehe, seien einige allgemeine Erkenntnisse zusammengefaßt.

2.3.1 Datenschutz als „technisches" Recht?

Das Datenschutzrecht ist vielfach als eine „technische" Rechtsmaterie aufgefaßt worden; manche meinen sogar, es sei nur die Übersetzung technischer Regeln in Rechtsnormen. Daher werden die vom BDSG den speichernden Stellen auferlegten Pflichten von vielen nur als lästige Formalien angesehen, die Kosten und Mühe verursachen und die man möglichst schnell ein für allemal „erledigen" müsse.

Tatsächlich erweist sich die Verwirklichung der formalen Gebote über Dateienregister und Veröffentlichungen (im öffentlichen Bereich) wie über Benachrichtigungen (im nicht-öffentlichen Bereich) und Auskünfte (in allen Bereichen) als aufwendig und schwierig. Auf der sorgfältigen Erfüllung dieser Pflichten muß aber beharrt werden — nicht aus engherzigem Formalismus heraus, sondern weil diese Vorschriften den Sinn haben, die Informationsverarbeitung *transparent* zu machen und dem Bürger die Wahrnehmung seiner Rechte zu ermöglichen oder zu erleichtern. Auch die Vorschriften zur Datensicherung werden mißverstanden, wenn man sie als Transformation vermeintlich technischer Regeln auffaßt; auch in ihnen spiegeln sich inhaltliche Entscheidungen des Gesetzgebers zum Schutze privater Rechte.

Ich habe auf verschiedene Weise versucht, Verständnis für solche Überlegungen zu verbreiten, und mich dabei nicht auf allgemeine Aussagen beschränkt, sondern detaillierte Hinweise und Informationen (zum Beispiel zu den Anmeldungen zum Dateienregister) gegeben.

Es liegt auf der Hand, daß über zahlreiche Fragen der praktischen Umsetzung des Gesetzes in technische und organisatorische Maßnahmen noch intensiv gerungen werden muß. Für die Dienststelle des Bundesbeauftragten ergibt sich hier eine umfangreiche Beratungsaufgabe. Da die Beratung in der Regel zu einem Einvernehmen über die datenschutzgerechte Ausgestaltung führen dürfte, werde ich von meinem Beanstandungsrecht voraussichtlich nur in seltenen Fällen Gebrauch machen müssen.

2.3.2 Umsetzung der allgemeinen Vorschriften in bereichsspezifische Datenschutzregeln

Wer die Datenschutzgesetze als bloß formal-technisches Recht ansieht, verkennt noch einen anderen wesentlichen Aspekt. Das Datenschutzrecht stellt einen ersten Teil eines neuen Rechtsgebiets dar, nämlich des Informationsrechts. Seine Schaffung beruht auf der Erkenntnis, daß die Sammlung, Speicherung und Übermittlung von Informationen rechtlich als Eingriffe in die Rechtssphäre der Betroffenen angesehen werden müssen und daher einer gesetzlichen Ermächtigungsgrundlage bedürfen. § 3 BDSG hat den im Verwaltungsrecht seit langem ausgeprägten Grundsatz vom „Vorbehalt des Gesetzes" auf das Informationswesen übertragen. Das neue Gesetz nötigt jeden, der Informationen über Personen verarbeitet, sich, den Betroffenen und der Öffentlichkeit Rechenschaft über die Rechtmäßigkeit dieser Informationsverarbeitung abzulegen.

Dieser Rechtfertigungsdruck des Gesetzes hat sich bereits in der ersten Zeit nach seinem Inkrafttreten deutlich bemerkbar gemacht. Freilich ist vielfach nur defensiv auf Einzelkritik reagiert worden. Viele Stellen wollen es genügen lassen, wenn sich irgendwo im geltenden Recht eine Bestimmung findet, die auf Informationen der betreffenden Art verweist. Die „Erforderlichkeit" der Datenverarbeitung und ihrer einzelnen Erscheinungsformen muß aber sorgfältiger und in größeren Zusammenhängen überprüft werden; dies ist eine zumindest mittelfristige Aufgabe, die noch lange über die Erfüllung der forma-

len Pflichten hinaus besteht. Überkommenes Recht muß Stück für Stück daraufhin untersucht werden, ob es unter den strengeren Voraussetzungen heutigen Datenschutzverständnisses noch die Grundlage für Speicherung und Übermittlung von Daten darstellen kann.

Dabei wird es zum einen darauf ankommen, abgestimmte Interpretationen der geltenden gesetzlichen Vorschriften zustande zu bringen. Dies ist das Ziel zahlreicher Besprechungen, die ich mit Bundesbehörden durchführe. Es gilt also zunächst, die Generalklauseln der Aufgaben- und Befugnisnormen (z. B. für die Polizeibehörden und den Verfassungsschutz) auf konkrete Praktiken der Informationsverarbeitung anzuwenden. Auch da, wo das Gesetz sehr allgemeine Formulierungen enthält, ist bei entsprechender Kooperationsbereitschaft der speichernden Stellen die Festlegung von Richtlinien künftiger Verwaltungspraxis möglich, die den Datenschutzaspekten besser Rechnung tragen als bisherige Verfahren.

Häufig wird aber diese Methode nicht weit genug tragen. Dann muß an den Gesetzgeber appelliert werden, bereichsspezifische Datenschutzbestimmungen zu erlassen. So ist es zum Beispiel beim Meldewesen, bei der Sozialverwaltung und — soweit erkennbar — auch bei der polizeilichen Informationssammlung. Mit Verwaltungsvorschriften allein kann in diesen Bereichen letztlich keine datenschutzgerechte Handlungsweise gewährleistet werden. Ich habe mich im Rahmen meiner rechtspolitischen Aufgabe für entsprechende Initiativen eingesetzt.

2.3.3 Verwaltungsbereiche, in denen besonders schwierige Datenschutzprobleme bestehen

In einigen Bereichen der öffentlichen Verwaltung sind die materiellen Datenschutzprobleme besonders schwierig, weil andere Interessen von hohem Rang entgegenstehen. So liegt es bei den Sicherheitsbehörden (vgl. dazu 3.4). Eine Weiterentwicklung des Datenschutzrechts scheint mir für diesen Bereich dringend erforderlich. Aber auch auf ganz anderen Gebieten besteht Regelungsbedarf. So sind sowohl Natur- wie Sozialwissenschaftler durch datenschutzrechtliche Bedenken gegen wissenschaftliche Datenerhebung und -auswertung erheblich verunsichert. Mit starken Auskunftsinteressen sehen sich auch die Träger der Sozialverwaltung konfrontiert, die das Sozialgeheimnis bewahren wollen (dazu 3.5).

Nach meinen Erfahrungen kann allerdings keineswegs gesagt werden, daß Risiken für private Rechte ausschließlich oder vornehmlich durch Datenverarbeitung von Staat und Kommunen entstehen. Auch andere Organisationen — seien es private Unternehmen oder Vereine und Verbände — sind nicht dagegen gefeit, den Datenschutz geringer zu achten als nach dem Gesetz vorgeschrieben. Die große Zahl der Eingaben, die sich mit Kreditauskunfteien und Versicherungsunternehmen beschäftigen, zeigt deutlich, daß die Bürger ihre Freiheit auch durch private Stellen gefährdet sehen. Erfahrungen aus dem öffentlichen Bereich sind auch für den nicht-öffentlichen von Bedeutung (und umgekehrt), die Forderung nach mehr Offenheit gegenüber den Betroffenen richtet sich an den einen wie an den anderen Bereich.

2.3.4 Flankierende Maßnahmen

Das Datenschutzrecht stellt nur einen Ausschnitt aus dem Schutz von Individualrechten bei der Informationsverarbeitung dar, und die gesetzliche Bestimmung des Anwendungsbereiches der Datenschutzgesetze, vor allem der Dateibegriff, wird von Betroffenen und publizistischen Beobachtern selbstverständlich nicht in den Feinheiten nachvollzogen. So wird es dem Datenschutzrecht angekreidet, wenn Persönlichkeitsverletzungen in benachbarten Bereichen mit den Mitteln des BDSG und der Landesdatenschutzgesetze nicht abgewehrt werden können. Defizite in diesem Randbereich entmutigen auch diejenigen, die sich im Anwendungsbereich der Datenschutzgesetze um eine strenge Handhabung bemühen.

So wird es vielfach als Mangel des Datenschutzrechts (im weiteren Sinne) angesehen, daß die Art und Weise der Daten*erhebung* im wesentlichen — von § 9 Abs. 2 BDSG abgesehen — ungeregelt geblieben ist, so daß hier auf allgemeine verfassungsrechtliche Grundsätze, wie sie von der Rechtsprechung teilweise konkretisiert worden sind, zurückgegriffen werden muß. Als besonders ärgerlich werden Gefährdungen oder Verletzungen des Persönlichkeitsrechts empfunden, die auf mangelnder Sorgfalt bei der *Übermittlung* beruhen. So ist es vorgekommen und kommt immer wieder vor, daß personenbezogene Daten von hohem Geheimhaltungsgrad (zum Beispiel Einkommenszahlen, Angaben über körperliche Behinderung, Mitteilungen über ein Ehescheidungsverfahren) in unzureichender Weise gegen Kenntnisnahme Dritter geschützt werden. Ein betrieblicher Datenschutzbeauftragter hat mir berichtet, daß in seinem Unternehmen zweimal Briefe öffentlicher Stellen eingegangen sind, in denen vertrauliche, nur für die Personalabteilung bestimmte Rückfragen in persönlichen Angelegenheiten von Mitarbeitern des Unternehmens enthalten waren, ohne daß dieser Inhalt äußerlich in irgendeiner Weise erkennbar gewesen wäre. Die Schreiben sind daher in der Poststelle geöffnet worden und konnten von Unbefugten eingesehen werden. Es liegt auf der Hand, daß sich jemand, der sich in einem Betrieb für die Durchsetzung von Datenschutzvorschriften einsetzt, durch solche Nachlässigkeiten beeinträchtigt fühlt. Für diese Beurteilung spielt es keine Rolle, ob die unangemessene Form des Versandes eine „Übermittlung aus einer Datei" darstellt oder nicht.

Bisweilen geschieht es sogar, daß zu schützende personenbezogene Daten in unverschlossenen Briefen oder auf offenen Postkarten verschickt werden. Soweit die allgemeinen Voraussetzungen der Anwendung des BDSG gegeben sind, ist in solchen Fällen das Datengeheimnis (§ 5 Abs. 1 BDSG) verletzt, das es den „bei der Datenverarbeitung beschäftigten Personen" untersagt, geschützte personenbezogene Daten unbefugt „zugänglich zu machen". Aber auch wenn diese Voraussetzungen nicht gegeben sind,

ist der Schutz personenbezogener Daten durch Wahl der richtigen Übermittlungsform als flankierende Maßnahme zum Datenschutz im engeren Sinne nachdrücklich zu empfehlen.

Welche Vielfalt von Verstößen gegen Sinn und Geist des Persönlichkeitsschutzes im Informationswesen möglich ist, zeigt auch ein anderes Beispiel: Die Registrierung von Nichtwählern. Mir war berichtet worden, daß eine Gemeindebehörde politischen Parteien Listen der Einwohner zur Verfügung gestellt habe, die ihr Wahlrecht nicht ausgeübt hätten. Schon die Zusammenstellung einer solchen Liste wäre nach § 9 Abs. 1 BDSG und den entsprechenden Bestimmungen der Landesdatenschutzgesetze unzulässig gewesen, ihre Übermittlung an eine Stelle außerhalb des öffentlichen Bereichs gemäß § 11 Satz 1 BDSG erst recht. Die Überprüfung ergab, daß die Behörde nicht in dieser Weise tätig geworden war; eine Aufzeichnung der Nichtwähler ist aber den politischen Parteien selbst möglich, wenn sie im Besitz der Wählerverzeichnisse sind und durch Beobachter im Wahllokal feststellen lassen, wer von seinem Wahlrecht Gebrauch macht. Die Wählerverzeichnisse werden den Parteien rechtmäßig überlassen (vgl. § 17 Abs. 1 Bundeswahlgesetz, § 18 Abs. 1 und Abs. 4 Bundeswahlordnung). Werden im Wahllokal die Namen oder auch nur die Nummern der Wähler aufgerufen, so kann jeder Beobachter, der die Abschrift des Wählerverzeichnisses besitzt, die Nichtwähler heraussuchen. Die Speicherung solcher Daten verstieße zwar gegen § 23 BDSG, doch wäre es angemessener, die aufgezeigte Gefahr für das Wahlgeheimnis durch eine Regelung im Wahlrecht auszuschließen.

2.3.5 Zur öffentlichen Diskussion über Datenschutzprobleme

Die öffentliche Auseinandersetzung um Fragen der Informationspolitik und Datenverarbeitung hat zu erheblicher Unruhe geführt. Zum Teil entsprachen die in der Öffentlichkeit verbreiteten Darstellungen über den Stand der Datenverarbeitung und die Ausbaupläne nicht den tatsächlichen Verhältnissen. Es ist aber müßig, über manchmal undifferenzierte oder unvollständige Berichterstattung zu klagen; die Medien sind nicht Verkündigungsorgane der staatlichen Stellen, sondern erfüllen die für das demokratische Gemeinwesen unverzichtbare Funktion der Kritik nach selbstgesetzten Normen. Selbst wenn dabei manches vergröbernd dargestellt wird und Ängste geweckt werden, die unbegründet sind — ich habe dies auch Journalisten gegenüber zum Ausdruck gebracht und mich meinerseits bemüht, möglichst genau zu formulieren —, so ist eine öffentliche Diskussion in jedem Fall zu begrüßen. Es bleibt den kritisierten Stellen unbenommen, ihre genauere Tatsachendarstellung und vielleicht besseren Argumente entgegenzusetzen. Manche düsteren Prognosen der journalistischen Beobachter erweisen sich gerade durch dieses Zusammen- und Gegenspiel im Rahmen der öffentlichen Diskussion als Vorhersagen, die sich selbst den Boden entziehen. Speziell zur Diskussion um das Meldewesen muß bemerkt werden, daß die Formulierungen des Gesetzentwurfes, den das Bundesministerium des Innern zunächst erarbeitet hatte, immerhin Anlaß zur Äußerung von Sorge gaben, da die möglicherweise mitgedachten Einschränkungen und Gegenmaßnahmen, die eine intensive Erfassung der Bürger durch das Meldewesen verhindern sollten, im Text nicht zum Ausdruck kamen.

Wir befinden uns in einem Stadium, in dem die Bürger den Stellen, die über moderne Informationsverarbeitungstechniken verfügen, auch eine weitgehende Ausnutzung dieser Möglichkeiten zutrauen. Wenn heute in der Fachliteratur oder der Tagespresse davon die Rede ist, daß ein groß angelegter Verbund von Datenbanken verschiedener Stellen — etwa der Versicherungswirtschaft, der Sozialversicherung und der Sicherheitsbehörden — *möglich* sei, so wird das von Bürgern vielfach so wahrgenommen, als sei es bereits *Realität*. Die Aufklärung solcher Vermutungen ist überaus mühsam und erfordert auch für den Fachmann einen erheblichen Aufwand. Selbst mit den Mitteln meiner Dienststelle ist es nicht immer möglich gewesen, kurzfristig die zur öffentlichen Diskussion gestellten Behauptungen aufzuklären.

Ich habe deshalb die Bundesbehörden immer wieder dazu aufgefordert, von sich aus der Öffentlichkeit darzustellen, welche Methoden der Datenverarbeitung tatsächlich praktiziert werden und welche Verbundsysteme bestehen. Dieser Appell richtet sich aber — über meine Kontrollzuständigkeit hinaus — auch an die anderen datenverarbeitenden Stellen. Nach meiner festen Überzeugung handeln sie gegen ihr eigenes Interesse, wenn sie die Bürger im Unklaren darüber lassen, welche Arten von Daten zu welchen Zwecken an welchen Stellen gespeichert und wohin sie übermittelt werden. Ausnahmen von der Offenlegung sind nur in geringem Umfang vertretbar, etwa für die Methoden der Geheimdienste; die Ausnahmen von der Veröffentlichungs- und Auskunftspflicht nach § 12 Abs. 2 und § 13 Abs. 2 BDSG sind meines Erachtens schon zu weit gezogen (dazu 3.4.7.3).

Die Kenntnis der üblichen Informationswege — wenigstens in Umrissen — ist eine wichtige Voraussetzung für Verhaltenssicherheit, also ein konstitutives Element des Zusammenlebens der Menschen im Gemeinwesen. Man muß einerseits ungefähr wissen, welche Kontrollen staatliche und andere Stellen ausüben oder auszuüben vermögen, andererseits sich darauf verlassen können, daß eine Überwachung in anderen Bereichen und auf andere Weise nicht üblich ist und also nicht erwartet zu werden braucht — außer in besonderen Fällen wie der Verfolgung wegen strafbarer Handlungen. Es ist nicht selbstverständlich, daß ein Kreditgeber im vorhinein bei einem umfassenden Informationssystem Aufkünfte über den Kreditkunden einholt; es ist nicht selbstverständlich, daß die Polizei die Einhaltung jeder beliebigen Rechtsvorschrift mit allen verfügbaren technischen Mitteln überwacht. Es ist auch rechtlich — wegen des Übermaßverbotes — nicht zulässig, alle möglichen Kontrollmaßnahmen zu ergreifen. Es wäre schlimm, wenn jeder, der irgendetwas geheimhalten möchte, mit der vollen Ausnutzung aller technischen und organisatorischen Informationsmöglichkei-

ten der „Gegenseite" rechnen müßte. Selbst unter den an sich gesetzlich zugelassenen Informationserhebungen und -übermittlungen gibt es tatsächlich viele, die nicht praktiziert werden — sei es, weil der Aufwand zu groß wäre, sei es, weil die zuständigen Stellen selbst erkennen, daß ein Mehr an Überwachung ein Minus an Rechtsstaatlichkeit bedeuten kann.

Der Bürger hat jedenfalls Anspruch darauf zu erfahren, in welchem Umfang und unter welchen (verwaltungspraktischen) Voraussetzungen von solchen Möglichkeiten Gebrauch gemacht wird; er braucht sich nicht ständig auf das „Schlimmste" einzurichten. So gesehen, ist das Vorbild mancher Polizeidienststellen, vor Radarkontrollen ausdrücklich zu warnen, nachahmenswert.

3 Stand des Datenschutzes in ausgewählten Bereichen

3.1 Bestandsaufnahme der Datenverarbeitung in der Bundesverwaltung

Die Bundesverwaltung bedient sich seit weit mehr als einem Jahrzehnt der Datenverarbeitung, um der Vielzahl ihrer Aufgaben gerecht werden zu können. Die Datenverarbeitung hat sich als ein unentbehrliches und besonders wirksames Hilfsmittel für die Regierungs- und Verwaltungstätigkeit erwiesen. Durch ihren Einsatz werden nicht nur allgemeine Leistungsverbesserungen erzielt und die Wirtschaftlichkeit erhöht; DV-gestützte Planungs- und Entscheidungshilfen sind für die Regierungsarbeit in einem modernen Staatswesen wie dem unseren unverzichtbar geworden. Manche Verwaltungsleistungen, insbesondere Massen- und Routinearbeiten, sind heute ohne Einsatz der ADV schlechthin nicht mehr zu erbringen.

Demzufolge ist die Zahl der mit Hilfe der ADV erledigten öffentlichen Aufgaben auch in der Bundesverwaltung ständig gewachsen. Zur Zeit stehen der unmittelbaren Bundesverwaltung ohne den Bereich des Bundesministers der Verteidigung, jedoch einschließlich Bundesbahn und -post, ca. 80 Rechenzentren für weit über 100 Benutzer und Mitbenutzer zur Verfügung. In diesen Rechenzentren sind über 150 DV-Anlagen im Einsatz. Der Bundesminister der Verteidigung betreibt 24 Rechenzentren, in denen überwiegend administrative und wissenschaftliche Aufgaben bearbeitet werden; daneben bestehen weitere DV-Anlagen für Zwecke der militärischen Führung. Im System der sozialen Sicherung sind ca. 160 Rechenzentren eingerichtet. Sie werden betrieben von den 22 Rentenversicherungsträgern (darunter 18 Landesversicherungsanstalten für Arbeiter, die Bundesversicherungsanstalt für Angestellte und die Bundesknappschaft), den 96 Unfallversicherungsträgern (darunter 35 gewerbliche und 19 landwirtschaftliche Berufsgenossenschaften sowie 22 Ausführungsbehörden des Bundes, der Länder und Gemeinden), den 1 363 Trägern der gesetzlichen Krankenversicherung (darunter u. a. 280 Ortskrankenkassen, 890 Betriebskrankenkassen und 157 Innungskrankenkassen) sowie deren Verbänden.

Ein erheblicher Teil dieser Institutionen sind bundesunmittelbare Körperschaften des öffentlichen Rechts und unterliegt damit der Kontrolle des Bundesbeauftragten für den Datenschutz. Eine Reihe von Bundesbehörden bedient sich zur Erledigung der Automationsaufgaben — in einem Falle auch für die Personalverwaltung — der Rechenzentren privatrechtlich organisierter Unternehmen und Körperschaften, die mehrheitlich aus Bundesmitteln finanziert werden.

Aus der Sicht des Datenschutzes sind in erster Linie die Rechenzentren von Interesse, in denen personenbezogene Daten gespeichert und verarbeitet werden. Hier sind vor allem die Rechenzentren der Rentenversicherungs- und Unfallversicherungsträger sowie der Träger der gesetzlichen Krankenversicherung zu nennen, in denen zum Teil besonders sensible Daten verarbeitet werden. Ein ähnlich bedeutsames Feld bilden die Sicherheitsbehörden mit ihren zum Teil die Bundesverwaltung übergreifenden Informationssystemen (Bundeskriminalamt, Bundesamt für Verfassungsschutz, Bundesnachrichtendienst).

In diesen Zusammenhang gehören auch das Kraftfahrtbundesamt mit dem Kraftfahrzeugbestands- und dem Verkehrszentralregister, das Bundeszentralregister beim Generalbundesanwalt und das Bundesverwaltungsamt mit dem Ausländerzentralregister. Dem Bundesverwaltungsamt obliegen auch die Verwaltung der Ausbildungsdarlehen nach dem BAföG und die Führung der Personaldatei des Bundesministers des Innern.

Aus dem Bereich des Personalwesens sind ferner die beim Bundesamt für Finanzen geführten Dateien über Besoldung, Versorgung und Vergütung der Bundesbediensteten und die Personaldatenbank des Bundesministers der Finanzen hervorzuheben; beim Auswärtigen Amt besteht eine DV-gestützte Personaldatei, bei der Gesellschaft für Mathematik und Datenverarbeitung die Personaldatei des Bundesministers für Forschung und Technologie. Von besonderem Interesse aus der Sicht des Datenschutzes ist schließlich auch das Statistische Bundesamt mit einer Vielzahl personenbezogener Daten aus allen Lebensbereichen.

Nach Aufbau und Auswertung des beim Bundesbeauftragten für den Datenschutz zu führenden Dateienregisters wird eine genaue Bestandsaufnahme der Datenverarbeitung in personenbezogenen Aufgabengebieten der Bundesverwaltung möglich sein.

3.2 Allgemeine innere Verwaltung

Der Bereich der allgemeinen inneren Verwaltung umfaßt eine Fülle von Aufgaben unterschiedlichster Art. Sie liegen überwiegend bei den Ländern. Soweit der Bund Zuständigkeiten auf diesem Gebiet besitzt, werden sie insbesondere vom Bundesverwaltungsamt wahrgenommen. Hier werde ich im Jahre 1979 mit systematischen Kontrollen beginnen.

Im Berichtszeitraum sind einige datenschutzrechtliche Einzelfragen an mich herangetragen bzw. von mir aufgegriffen worden, die ich im folgenden behandle.

3.2.1 Wahlen

Nach § 13 der Bundeswahlordnung sind in das Wählerverzeichnis Familienname, Vorname, Geburtsdatum und Wohnung der Wahlberechtigten aufzunehmen. Das Wählerverzeichnis ist während eines bestimmten Zeitraumes vor jeder Wahl zur Einsicht durch jedermann auszulegen. Dadurch kann jeder wahlberechtigte Bürger prüfen, ob er selbst im Wählerverzeichnis aufgeführt ist und ob gegen die Aufnahme anderer Personen Bedenken bestehen. Über diese Zweckbestimmung hinaus läßt sich das Wählerverzeichnis aber auch benutzen, um zum Beispiel festzustellen, wann die Nachbarin geboren ist. Dieser datenschutzrechtliche Aspekt hat zu Überlegungen geführt, das Geburtsdatum in dem auszulegenden Wählerverzeichnis zu streichen. Erste Schritte in diese Richtung sind getan worden.

Auf Bundesebene ist auf meinen Vorschlag hin in die Europawahlordnung eine Bestimmung aufgenommen worden, wonach der Wahlberechtigte verlangen kann, daß die Angabe über den Tag seiner Geburt im auszulegenden Wählerverzeichnis während der Auslegungsfrist unkenntlich gemacht wird (§ 20 EuWO). Bayern ist noch einen Schritt weitergegangen und hat in der Landeswahlordnung vom 17. Mai 1978 bestimmt, daß für die Auslegung ein gesondertes Wählerverzeichnis ohne Angabe des Geburtstages zu verwenden ist. Ich bin sicher, daß diese Denkanstöße fortwirken und letztlich dazu führen werden, im gesamten Bundesgebiet so zu verfahren. Ich werde mich dafür einsetzen.

Ein schwieriges datenschutzrechtliches Problem bildet auch die Frage, ob und unter welchen Voraussetzungen den politischen Parteien Anschriften von Wahlberechtigten mitgeteilt werden dürfen. Die Regelung des § 18 Abs. 4 der Bundeswahlordnung, die eine Weitergabe des Wählerverzeichnisses innerhalb der Auslegungsfrist erlaubt, hat sich als unzulänglich erwiesen. Die Auslegungsfrist von 24 Tagen vor der Wahl ist zu kurz, um dann noch eine gezielte Wahlwerbung vorbereiten und durchführen zu können. Es sollte den politischen Parteien und anderen am Wahlkampf teilnehmenden Gruppen aber möglich sein, bestimmte Altersgruppen unter den Wählern in angemessener Zeit vor den Wahlen ansprechen zu können. Daher habe ich in meiner gutachtlichen Stellungnahme zum Entwurf eines Bundesmeldegesetzes vorgeschlagen, in ein künftiges Bundesmeldegesetz eine Bestimmung aufzunehmen, nach der die Meldebehörde Parteien und Wählergruppen bis zu sechs Monaten vor der Wahl Auskünfte über Personengruppen erteilen darf, für deren Zusammensetzung das Lebensalter des Betroffenen bestimmend ist. Damit die Belange des Datenschutzes gewahrt bleiben, dürfen die Geburtstage der Betroffenen dabei aber nicht mitgeteilt werden.

3.2.2 Meldewesen

Das Meldewesen ist der einzige Bereich der öffentlichen Verwaltung, der — von geringen Ausnahmen abgesehen — Daten über *alle* Bewohner des Bundesgebietes sammelt und für administrative Zwecke zur Verfügung hält. Schon dadurch ist dieser Verwaltungsbereich unter Datenschutzaspekten von besonderem Interesse. Gesetzliche Regelungen haben bisher nur die Länder erlassen; ein erheblicher Teil der die Praxis beherrschenden Regelungen ist überdies bis heute nur in Verwaltungsvorschriften enthalten, also nicht aus einer parlamentarischen Beratung hervorgegangen und — mangels Rechtsnormqualität — für das Außenverhältnis dem Bürger gegenüber nicht verbindlich.

Dem Bund steht die Kompetenz zum Erlaß eines Rahmengesetzes über das Meldewesen zu (Artikel 75 Nr. 5 GG). Versuche, von dieser Kompetenz Gebrauch zu machen, sind bisher gescheitert. Zuletzt hat der damalige Bundesminister des Innern Ende des Jahres 1977 den Entwurf eines Bundesmeldegesetzes vorbereitet. Er wurde in der Öffentlichkeit heftig kritisiert; der Minister zog ihn daraufhin zurück. Als Grundlage der weiteren Beratung und einer Expertenanhörung hat der Bundesminister des Innern eine gutachtliche Stellungnahme des Bundesbeauftragten für den Datenschutz erbeten und dazu die folgenden Fragen gestellt:

1. Wie beurteilen Sie — ausgehend vom Regierungsentwurf eines Bundesmeldegesetzes — aus der Sicht des Datenschutzes
   - 1.1. die Aufgabenstellung des Meldewesens, wie es sich in der historischen Entwicklung und nach heutiger Verwaltungspraxis darstellt,
   - 1.2. Umfang und Inhalt des zur Speicherung im Meldewesen vorgesehenen Datenkatalogs,
   - 1.3. die Einrichtung von Landesadreßregistern und deren Dateninhalt,
   - 1.4. die Datenübermittlung an andere Meldebehörden und sonstige öffentliche Stellen,
   - 1.5. die Auskunftserteilung an Dritte,
   - 1.6. die Sperrung und die Löschung von Daten?
2. Halten Sie weitergehende Regelungen über Rechte der Betroffenen für notwendig?
3. Welche sonstigen Maßnahmen können Sie zur Verbesserung des Datenschutzes im Meldewesen empfehlen?

Diese Fragen habe ich in einer gutachtlichen Stellungnahme nach § 19 Abs. 1 Satz 2 BDSG vom 15. Oktober 1978 beantwortet. Der Stellungnahme

ist ein ausformulierter Gesetzesvorschlag beigefügt, der die wesentlichen Ergebnisse meiner Überlegungen wiedergibt.

Die grundlegenden Überlegungen habe ich in der Anhörung, die das Bundesministerium des Innern am 20. und 21. November 1978 veranstaltet hat, sinngemäß etwa wie folgt vorgetragen:

— Das Meldewesen bedarf einer bereichsspezifischen Datenschutzregelung.

— Das Meldewesen muß bürgerfreundlich gestaltet werden.

  Hinter dieser Formel verbergen sich unterschiedliche, teilweise durchaus divergierende Ziele. Für manche ist „Bürgerfreundlichkeit" gleichbedeutend mit „Effektivität" (im weiteren Sinne auch: Einfachheit, Übersichtlichkeit, kurz: „Bequemlichkeit" des Meldewesens, Vermeidung von Mehrfachanfragen und Mehrfachspeicherung). Andere hingegen verstehen darunter eine andere Qualität von Verwaltung, nämlich eine — in bezug auf die Erfassung der Bürger — freiheitlichere, auf Kompetenzverteilung bedachte und damit die Geheimhaltungsinteressen der Bürger besser wahrende Form von Administration. „Dienst am Bürger" kann die Verwaltung auch durch Bereitstellung von Auskünften über andere Bürger leisten; die Auskunftsbereitschaft der Meldebehörden für andere Behörden und für interessierte Dritte ist eine Grundlage schneller und zuverlässiger Erledigung aller möglichen Verwaltungsvorgänge in Staat und Wirtschaft und beim einzelnen.

— Der Zielkonflikt zwischen Effektivität und Freiheitlichkeit der Verwaltung kann und darf nicht so gelöst werden, daß eines der Ziele zu Lasten des anderen verabsolutiert wird. Die beiden Zielgruppen müssen möglichst weitgehend miteinander in Einklang gebracht werden. Maßstab der Gestaltung muß selbstverständlich die Verfassung sein, die in Artikel 1 Abs. 3 und Artikel 20 Abs. 3 GG die Bindung auch des Gesetzgebers an die Grundrechte und die verfassungsmäßige Ordnung vorschreibt. Auch die verfassungsgerichtliche Judikatur ist selbstverständlich zu berücksichtigen, ebenso die neuere Erkenntnis, daß es einen Eingriff in die Rechtssphäre des einzelnen bedeuten kann, wenn Informationen über ihn gesammelt und weitergegeben werden (diese Ansicht hat sich der Gesetzgeber im BDSG zu eigen gemacht und folgerichtig vorgeschrieben, daß solche Eingriffe nur mit Einwilligung des Betroffenen oder auf einer gesetzlichen Grundlage zulässig sind).

— Bei der Abwägung der verschiedenen Positionen geht es im Kern immer auch um die Abwägung von Grundrechten verschiedener Beteiligter gegeneinander. Der eine will einen Anspruch durchsetzen, der andere möchte sich abschirmen — wie soll die Behörde in einem solchen Fall ihr Wissen nutzbar machen? Der Staat will seinen Strafanspruch gegen einen Verdächtigen realisieren, dieser wehrt sich gegen die Verwendung von Informationen, die aus anderen Zusammenhängen stammen — wie soll entschieden werden?

  Die Ansicht, Rechtsstaatlichkeit gebiete, daß die Verfolgung von Rechtsansprüchen unbedingt Vorrang vor dem Geheimhaltungsinteresse des einzelnen verdiene, ist falsch. Unser Recht kennt viele Regeln, die es erschweren oder unmöglich machen, einen an sich begründeten Anspruch durchzusetzen; auch Strafanspruch und Steueranspruch des Staates können nach geltendem Recht häufig nicht durchgesetzt werden, weil Freiheitsrechte von Bürgern entgegenstehen. Ein Staat, der alle materiellen Ansprüche „hundertprozentig" durchsetzen wollte, wäre kein „hundertprozentiger" Rechtsstaat, sondern ein Zwangsstaat.

— Rationalisierung und Vereinfachung der Verwaltung haben bei der Abwägung mit Freiheitspositionen einen geringeren Stellenwert. Um des Datenschutzes willen kann es geboten sein, von der Mehrfachnutzung gesammelter Informationen abzusehen und statt dessen dem Bürger zuzumuten, dieselben Angaben verschiedenen Stellen zu machen.

Ich habe in der Anhörung ferner sinngemäß ausgeführt:

  Die öffentliche Kritik an dem früher vorgelegten Entwurf eines Bundesmeldegesetzes lief darauf hinaus, daß die Bundesregierung dazu ansetze, ein Überwachungssystem größten Umfanges zu etablieren oder — soweit es schon vorhanden sei — nachträglich zu legalisieren. Diese Kritik war falsch, weil derartige Pläne nicht bestanden. Aber die Ängste der Bürger waren verständlich, weil es immerhin die Tendenz gab, aus dem Meldewesen ein Informationssystem über die Einwohner zu machen, das in vieler Hinsicht ausbaufähig gewesen wäre. Mag es auch in der öffentlichen Diskussion um dieses „Einwohnerwesen" zu erheblichen Übertreibungen gekommen sein — der Vorwurf war berechtigt, daß der Gesetzestext eine extensive Informationssammlung und -übermittlung nicht ausschloß. Den Gesetzesverfassern war es zumindest nicht gelungen, Gegenmaßnahmen in zweifelsfreier Weise zu formulieren. Dies darf sich nicht wiederholen. Es darf gar nicht erst der Verdacht aufkommen, mit dem Meldewesen werde eine umfassende Registrierung von Informationen über die Bürger und der ganz große Verbund öffentlicher Datenbanken angestrebt.

Als Formulierungshilfe habe ich den bereits erwähnten Gesetzesvorschlag ausgearbeitet. Meine Überlegungen lassen sich wie folgt zusammenfassen:

— Nach der Kompetenznorm des Artikels 75 Nr. 5 GG darf der Bund vom Ansatz her die Speicherung derjenigen Einwohnerdaten regeln, die sich auf den Wohnsitz und den Aufenthalt eines Einwohners beziehen. Der Entwurf muß daher neu konzipiert werden. Den Meldebehörden obliegt im Kern die Feststellung der Identität und der Wohnung oder des Aufenthalts der Einwohner. Ihnen können darüber hinaus Tätigkeiten gesetz-

lich übertragen werden, die in konditionalem Zusammenhang mit der Personen- oder Aufenthaltsfeststellung stehen; die dafür notwendigen Daten dürfen erfaßt und verarbeitet werden. Ein solcher Zusammenhang besteht insbesondere für Personalausweise, Wählerverzeichnisse, Lohnsteuerkarten und die Wehrüberwachung.

— Der Datenkatalog der Anlage zu dem bisherigen Gesetzentwurf muß grundlegend überarbeitet werden. Für das Meldewesen selbst sind an sich nur Grunddaten wie Name, Geschlecht, Geburtsdatum und Anschrift notwendig. Für die Erfüllung weiterer zugewiesener Aufgaben dürfen auch Spezialdaten gespeichert werden; sie dürfen aber nur mit den Grunddaten, nicht mit anderen Spezialdaten zusammengeführt werden. Besonders empfindliche Daten müssen neutralisiert werden. Beispielsweise genügt anstelle der Angabe bestimmter Wahlausschlußgründe der Hinweis, daß ein solcher Grund vorhanden ist; der Grund im einzelnen ist nicht zu speichern.

— Der zulässige Umfang der Datenerhebung für das Meldewesen und die zulässigen regelmäßigen oder besonderen Übermittlungen von Daten zwischen Meldebehörden oder zwischen Meldebehörden und anderen Behörden sind gesetzlich festzulegen.

Im einzelnen muß gelten:

Die Mitteilung des Wohnungswechsels an die Meldebehörde des früheren Wohnorts oder an andere für sonstige Wohnungen des Betroffenen zuständige Meldebehörden ist datenschutzrechtlich unbedenklich.

Regelmäßige Datenübermittlungen an andere öffentliche Stellen müssen nach Anlaß, Inhalt, Empfänger und Verwendungszweck im Meldegesetz des Bundes oder in den Landesmeldegesetzen festgelegt werden.

Grunddaten dürfen an andere öffentliche Stellen bei Bedarf stets übermittelt werden. Die Übermittlung darüber hinausgehender Daten ist nur in Ausnahmefällen und unter bestimmten, gesetzlich festgelegten Voraussetzungen zulässig.

An öffentlich-rechtliche Religionsgesellschaften dürfen nur Grunddaten ihrer Mitglieder übermittelt werden, darüber hinausgehende Daten nur bei Vorliegen eines öffentlichen Interesses aus staatlicher Sicht.

— Auskünfte an Private über Name und Anschrift (einfache Auskünfte) sind immer zulässig. Der betroffene Einwohner kann diese Daten sperren lassen, wenn er ein berechtigtes Interesse darlegt.

Darüber hinausgehende Daten (erweiterte Auskunft) dürfen an Dritte nur weitergegeben werden, soweit diese ein berechtigtes Interesse gerade an diesen Daten geltend machen können; der Betroffene kann die erweiterte Auskunft ohne weitere Voraussetzungen sperren lassen. (Dieser Punkt war in der Anhörung des Innenministeriums besonders umstritten; gegen ihn haben die Vertreter der Wirtschaft Einwendungen erhoben.)

Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) darf nur im öffentlichen Interesse erteilt werden.

— Die dem betroffenen Einwohner zustehenden Rechte sind einzeln zu regeln, insbesondere:
  - gebührenfreie Auskunft
  - Berichtigungsanspruch
  - Löschungsanspruch
  - Anspruch auf Übermittlungs- und Auskunftssperren
  - Anspruch auf Unterrichtung über an Dritte erteilte erweiterte Auskünfte.

— Daten, die zur Aufgabenerfüllung der Meldebehörden nicht mehr erforderlich sind, sind nicht nur zu sperren, sondern zu löschen. Für Grunddaten wird eine Löschungsfrist von 30 Jahren vorgeschlagen.

— Landesadreßregister bedürfen einer Rechtsgrundlage im Gesetz. Zur Beurteilung ihrer Notwendigkeit und Zwecke fehlen noch ausreichende Entscheidungsgrundlagen. Eine bundesgesetzliche Regelung, die die Errichtung von Landesadreßregistern zwingend vorschriebe, wäre daher problematisch. In jedem Fall müßten zugriffsberechtigte Behörden gesetzlich festgelegt sein. Unzulässig wäre die Zusammenfassung der Landesadreßregister durch landesübergreifende Online-Verbindungen.

3.2.3 Personalwesen

3.2.3.1 Personalinformationssysteme

Im Berichtsjahr habe ich erste Erkundungen darüber angestellt, wie personenbezogene Daten von Mitarbeitern der Bundesverwaltung durch Personaldienststellen verarbeitet werden. Eine Untersuchung vorhandener Personalinformationssysteme auf datenschutzgerechte Ausgestaltung war jedoch noch nicht möglich. Vorbereitungen für solche Untersuchungen sind getroffen.

3.2.3.2 Stellung des Personalrats

Es ist viel diskutiert worden, ob der Betriebsrat eines privatrechtlichen Unternehmens datenschutzrechtlich als Teil dieses Unternehmens oder als Dritter angesehen werden muß — von der Antwort hängt z. B. ab, ob Übermittlungen von Daten an den Betriebsrat einer besonderen gesetzlichen Ermächtigung bedürfen und ob der Datenschutzbeauftragte des Betriebes auch Aufsichtsbefugnisse über den Betriebsrat besitzt. Analog dieser Frage war für die öffentliche Verwaltung streitig, ob der Personalrat Dritter im Sinne des § 2 Abs. 3 Nr. 2 BDSG ist. Nach dieser Bestimmung ist Dritter jede Person oder Stelle außerhalb der speichernden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen des § 2 Abs. 3 Nr. 1

im Geltungsbereich des BDSG „im Auftrag" tätig werden.

Ich habe hierzu den Standpunkt vertreten, daß sich die Aufgaben und Befugnisse, die dem Personalrat gesetzlich zugewiesen sind, ausschließlich auf den internen Bereich der Dienststelle erstrecken, bei der die Personalvertretung gebildet worden ist. Daher ist die Personalvertretung als ein internes Organ der Dienststelle anzusehen, das an deren Willensbildung in innerdienstlichen Angelegenheiten beteiligt ist. Auf den Bereich der Dienststelle ist der Handlungsraum der Personalvertretung festgelegt und begrenzt. Das Bundesverfassungsgericht hat in einem Beschluß vom 31. August 1976 — 2 BvR 467/76 — ausdrücklich festgestellt, daß der (Haupt-)Personalrat keine eigene Rechtspersönlichkeit besitze, sondern eine öffentlich-rechtliche Organstellung im internen Verwaltungsaufbau habe; er stehe also dem Staat nicht gegenüber, sondern sei dort, eingebunden in die Verwaltung, Repräsentant der Bediensteten.

Danach kann der Personalrat nicht als Dritter im Sinne des § 2 Abs. 3 Nr. 2 BDSG angesehen werden, er ist vielmehr Teil der speichernden Stelle (§ 2 Abs. 3 Nr. 1 BDSG).

Aufgaben und Befugnisse des Personalrats, insbesondere der Informationsaustausch zwischen Dienststelle und Personalrat einschließlich etwaiger Schweigepflichten (siehe § 10 Bundespersonalvertretungsgesetz), sind durch das Personalvertretungsgesetz abschließend geregelt. Das BDSG ändert insoweit nichts an dem Verhältnis zwischen Dienststelle und Personalvertretung, sondern bringt für personenbezogene Daten in Dateien ausdrücklich den Gesichtspunkt des Datenschutzes zum Tragen, der für die Dienststelle wie für die Personalvertretung gleichermaßen verbindlich ist.

Dementsprechend bestimmt das BDSG in § 45, daß besondere Rechtsvorschriften des Bundes, soweit sie auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, den Vorschriften des BDSG vorgehen.

3.3 Statistik und Volkszählung

3.3.1 Möglichkeiten und Ziele der Kontrolle im Bereich der Statistik

Bei der Durchführung von Bundesstatistiken werden in großem Umfang personenbezogene Daten erhoben und gespeichert. Die Entscheidungsträger in Staat und Wirtschaft sind in immer stärkerem Maße auf umfassende, genaue und aktuelle Informationen über das soziale und wirtschaftliche Geschehen angewiesen. Dies hat zu einer wesentlichen Erweiterung und Verfeinerung des statistischen Erhebungsprogrammes geführt. Auch die Methoden der Datenanalyse sind, gestützt auf die automatische Datenverarbeitung, rasch fortgeschritten. Die Entwicklung statistischer Datenbanken, die auf nicht-aggregierten Datensätzen aufbauen und vielfältige Auswertungsmöglichkeiten eröffnen, verdient freilich aus der Sicht des Datenschutzes besonderes Interesse. Der Hinweis auf das gesetzlich verankerte Statistikgeheimnis genügt nicht mehr, um jede Besorgnis zu zerstreuen.

Sinn des Datenschutzes kann es nicht sein, die wissenschaftliche und technische Entwicklung aufzuhalten und den Aufbau von Informationsinstrumenten, die für ein besseres, vorausschauendes Handeln unentbehrlich sind, zu verhindern. Es kann allerdings auch nicht darum gehen, den Datenschutz des einzelnen den wachsenden Informationsbedürfnissen der Gesellschaft zu opfern. Worauf es vielmehr ankommt, ist die Entwicklung von rechtlichen, organisatorischen und technischen Modellen, die den Anspruch der Betroffenen auf Datenschutz und die vielfältigen Bedürfnisse an statistischer Information soweit wie möglich miteinander vereinbar machen.

Zwar trifft auch für die Statistik zu, daß eine hundertprozentige Sicherung gegen Mißbrauch nicht möglich ist. Nur unter der Voraussetzung, daß es gelingt, das Risiko so weit wie irgend möglich zu reduzieren, ist es aber gerechtfertigt, die Bürger zur Erteilung von Auskünften zu verpflichten; nur dann kann auch erwartet werden, daß die Bereitschaft zu vollständigen und zutreffenden Auskünften besteht, auf die die Statistischen Ämter ungeachtet der Rechtspflicht angewiesen sind.

Das Ziel meiner Kontrolltätigkeit ist es deshalb, auf eine absolut korrekte Einhaltung der Datenschutzvorschriften zu achten. Auch ein noch so überzeugend vorgetragener Informationswunsch darf nicht zu einem „großzügigen" Umgang mit der statistischen Geheimhaltung führen — selbst wenn damit der Vorwurf bürokratischer Kleinlichkeit provoziert wird. In dieser Grundeinstellung bestehen nach meinen bisherigen Erfahrungen keine Meinungsverschiedenheiten mit den für die Bundesstatistiken verantwortlichen Instanzen der Verwaltung. Diese Übereinstimmung zu sichern und in der Praxis auszubauen, betrachte ich als die entscheidende Voraussetzung dafür, daß die Bemühungen um eine den veränderten sozialen und technischen Bedingungen gerecht werdende Fortentwicklung des Statistikrechts und der statistischen Praxis von der Öffentlichkeit verstanden und akzeptiert werden.

Ich hatte bereits im ersten Jahr meiner Tätigkeit vielfältige Gelegenheit, diese Grundsätze in der Praxis zur Geltung zu bringen. Die Erhebung und die Aufbereitung von Daten im Rahmen der Bundesstatistiken liegen zwar überwiegend in der Verwaltungszuständigkeit der Länder. Eingaben aus diesem Bereich habe ich daher, teilweise verbunden mit einer Stellungnahme, an die für die Kontrolle des Datenschutzes in den Ländern zuständigen Organe weitergereicht. Soweit jedoch die Festlegung der Erhebungsprogramme, die in den Gesetzen meist nur in allgemeiner Form beschrieben sind, beim Statistischen Bundesamt liegt, kann ich von meinen Kontrollbefugnissen Gebrauch machen. In zwei Fällen haben meine Überprüfungen zu einer Beanstandung nach § 20 BDSG geführt. Ich habe ferner die Gelegenheit wahrgenommen, zu Gesetzgebungsvorhaben auf dem Gebiet der Statistik Stellung zu nehmen, und dabei eine Reihe von Empfehlungen zur Verbesserung des Datenschutzes gegeben.

3.3.2 Beanstandungen bei Erhebungen nach dem Hochschulstatistikgesetz

Mehrere Hochschulangehörige haben sich durch eine bundesweit durchgeführte „Erhebung über wissenschaftliches und künstlerisches Personal an Hochschulen" in ihrer Privatsphäre beeinträchtigt gesehen und bei mir angefragt, ob sie zur Auskunft verpflichtet seien. Meine Prüfung hat ergeben, daß das vom Statistischen Bundesamt festgelegte Erhebungsprogramm in drei Punkten nicht durch das Hochschulstatistikgesetz (BGBl. I 1977 S. 1473), auf dessen Grundlage die Erhebung durchgeführt wurde, gedeckt war. Insoweit war es deshalb unzulässig, die Hochschulangehörigen unter Androhung von Bußgeldern zur Auskunftserteilung aufzufordern. Unzulässig waren die Fragen nach

1. der von der Hochschule vergebenen Personalnummer des Befragten,
2. den Namen anderer Hochschulen, an denen der Befragte einer weiteren Beschäftigung nachgeht, und
3. dem Bestehen weiterer anzeigepflichtigen Beschäftigungen jeglicher Art.

Die Personalnummer zählt nicht zu den „Angaben zur Person", die nach § 7 Nr. 1 Hochschulstatistikgesetz erhoben werden dürfen. Sie gehört weder zum Namen noch ist sie ein persönliches Merkmal des Betroffenen. Personalnummern und ähnliche Identifizierungsmerkmale werden vom Gesetzgeber als ein eigener Erhebungstatbestand betrachtet; § 55 Bundesausbildungsförderungsgesetz wurde eigens ergänzt (durch Artikel 1 Nr. 11 des Änderungsgesetzes vom 14. November 1973, BGBl. I S. 1637), um zu ermöglichen, daß neben dem Namen auch die Förderungsnummer erhoben wird; entsprechend führt § 6 Abs. 3 Mikrozensusgesetz vom 15. Juli 1975 (BGBl. I S. 1909) „Namen, Anschrift und ein Personenkennzeichen" als getrennte Tatbestände auf.

§ 7 Nr. 3 Hochschulstatistikgesetz erlaubt die Erhebung von „Zahl und Art weiterer Beschäftigungsverhältnisse", mithin eine nur zahlen- und gattungsmäßige Erfassung. Die unzulässige Aufforderung, andere Hochschulen, an denen eine Beschäftigung ausgeübt wird, namentlich zu bezeichnen, berührt die schutzwürdigen Belange der Auskunftspflichtigen insbesondere dadurch, daß das Hochschulstatistikgesetz in § 19 Abs. 3 den erhebenden Hochschulen die Verwendung der Daten für „verwaltungsinterne Zwecke", also beispielsweise unter dienstrechtlichen Gesichtspunkten, gestattet.

Ähnliche Komplikationen entstehen durch die Frage, ob „eine weitere anzeigepflichtige Beschäftigung jeglicher Art" ausgeübt wird, die ebenfalls nicht durch den gesetzlichen Tatbestand „Zahl und Art weiterer Beschäftigungsverhältnisse" gedeckt ist. Sie setzt die Befragten unter Druck, weil sie sich unter Umständen einer dienstrechtlichen Verfehlung (Nichtanzeige der Nebenbeschäftigung) bezichtigen müssen.

Bei der ebenfalls auf dem Hochschulstatistikgesetz beruhenden „Erhebung über Prüfungskandidaten" waren die Fragen über die Berechtigung zum Hochschulstudium zu beanstanden, weil sie weder zu den „Angaben zur Person" noch zu den im Gesetz vorgesehenen Angaben zum „Studienverlauf" gerechnet werden können.

Schon vor der Aufnahme meiner Tätigkeit hatte der Hessische Datenschutzbeauftragte beanstandet, daß in die Erhebung für Personal an Hochschulen das gesamte Personal im höheren Dienst einbezogen wurde, obwohl § 3 Nr. 4 Hochschulstatistikgesetz ausdrücklich die Einbeziehung nur eines bestimmten Teiles des höheren Dienstes, nämlich insbesondere des wissenschaftlichen und künstlerischen Personals, vorsieht (vgl. VII. Tätigkeitsbericht des Hess. Datenschutzbeauftragten vom 21. Dezember 1978 zu 6.4).

Die Beanstandungen sind vom fachlich zuständigen Bundesminister für Bildung und Wissenschaft in vollem Umfang für berechtigt erklärt worden. Das Statistische Bundesamt wurde entsprechend angewiesen. Es ist Angelegenheit der Länder, für eine Löschung aller ohne gesetzliche Grundlage erhobenen personenbezogenen Daten zu sorgen.

Die Verantwortung für den Inhalt des Erhebungsprogramms liegt beim Statistischen Bundesamt. Es wird dabei nach § 21 Hochschulstatistikgesetz vom Ausschuß für die Hochschulstatistik beraten, in dem insbesondere die Hochschulen und wissenschaftliche Organisationen vertreten sind. Es besteht der Eindruck, daß bei der Festlegung der Erhebungsprogramme für die genannten Statistiken fachliche Gesichtspunkte, konkret: die Informationsinteressen der Hochschuladministration, so stark im Vordergrund gestanden haben, daß die Prüfung der Geestzmäßigkeit daneben vernachlässigt wurde.

Ich empfehle, bei der Aufstellung statistischer Fragekataloge den datenschutzrechtlichen Anforderungen stärkere Bedeutung beizumessen. In der Statistik muß ebenso wie bei jeder anderen Verarbeitung personenbezogener Daten der Grundsatz gelten, daß der Datenschutz nicht erst bei der Geheimhaltung beginnt, sondern schon bei der Erhebung und Erfassung der personenbezogenen Daten.

3.3.3 Verwendung statistischer Einzelangaben für Verwaltungszwecke

Die im Zusammenhang mit Erhebungen auf der Grundlage des Hochschulstatistikgesetzes erhobenen Beanstandungen werfen auch ein kritisches Schlaglicht auf eine Besonderheit der Hochschulstatistik. Nach § 19 Abs. 3 dürfen die meisten der nach dem Gesetz erhobenen Einzelangaben „von den jeweils zuständigen Erhebungsstellen für deren verwaltungsinterne Zwecke auch mit Namen und Anschrift des Auskunftspflichtigen verwendet werden. Wechseln die Auskunftspflichtigen die Schule oder Hochschule, so dürfen die Einzelangaben mit Namen und Anschrift an die neue Schule oder Hochschule für deren verwaltungsinterne Zwecke weitergeleitet werden". Die auf statistischer Rechtsgrundlage erhobenen Angaben dürfen also nicht nur statistisch ausgewertet, sondern auch als Grundlage für Verwaltungsentscheidungen im Verhältnis zur einzelnen auskunftspflichtigen Person genutzt werden.

Eine solche Vermischung von Aufgaben der Statistik und des Verwaltungsvollzugs halte ich für proble-

matisch. Meine Bedenken rühren zunächst daher, daß Stellen, die für den Vollzug von Verwaltungsaufgaben zuständig sind, Angaben zur Kenntnis erhalten, deren Erhebung und Speicherung aus der Sicht ihrer Aufgaben nicht erforderlich ist und die sie daher vom Betroffenen auf direktem Wege nicht erheben könnten — so die Angaben der Studenten zum Berufsziel sowie zur Ausbildung ihrer Eltern und deren Stellung im Beruf. Die oben genannten Daten aus dem Personalwesen könnten nur unter bestimmten Bedingungen und jedenfalls nicht unter Bußgeldandrohung gefordert werden. Es sollte auch nicht übersehen werden, daß bei einer Personalerhebung unter statistischen Vorzeichen das Mitbestimmungsrecht der Personalvertretungen in bezug auf den „Inhalt von Personalfragebogen" (vgl. § 75 Abs. 3 Nr. 8 Bundespersonalvertretungsgesetz) umgangen wird.

Die mit dem Nutzungsrecht der Hochschulverwaltung an den statistischen Daten verbundenen Komplikationen zeigten sich auch bei der Eingabe eines Bürgers gegen eine von einem Hochschulinstitut durchgeführte Erhebung. In dem Begleitschreiben zum Fragebogen hieß es: „Es wird Ihnen vielleicht aufgefallen sein, daß wir auf den meisten Fragebogen ihre Matrikelnummer mit erheben. Wir tun dies, um Ihnen ein wiederholtes Abfragen Ihrer Sozialdaten (Alter, Geschlecht, Hörerstatus) zu ersparen".

Der Fall wirft die Frage auf, ob Einzelangaben, die im Rahmen der Hochschulstatistik erhoben worden sind, von den Einrichtungen der Hochschule außer für administrative auch für wissenschaftliche Zwecke verwendet werden dürfen. Die Frage ist zu verneinen. § 19 Abs. 2 Satz 2 Hochschulstatistikgesetz läßt zwar unter gewissen Voraussetzungen eine Weiterleitung von Einzelangaben für wissenschaftliche Zwecke zu, behält diese Befugnis jedoch den statistischen Ämtern vor. Den Hochschulen wird die Verwendung der Einzelangaben lediglich „für deren verwaltungsinterne Zwecke" (§ 19 Abs. 3) gestattet.

Wenn das Gesetz hier nicht schlechthin von eigenen oder internen, sondern ausdrücklich von „verwaltungsinternen" Zwecken spricht, dann um deutlich zwischen dem administrativen und dem wissenschaftlichen Bereich der Hochschule zu unterscheiden. Die Hochschulverwaltung darf deshalb Einzelangaben anderen Organisationseinheiten der Hochschule für wissenschaftliche Zwecke nur dann aushändigen, wenn jeder einzelne Betroffene eingewilligt hat.

Aus Zuständigkeitsgründen konnte ich der Angelegenheit nicht weiter nachgehen. Wegen der großen Bedeutung, die ich der Wahrung des Statistikgeheimnisses beimesse, habe ich meine Auffassung jedoch dem Bundesminister für Bildung und Wissenschaft mitgeteilt und nahegelegt, den Hochschulen die komplizierte datenschutzrechtliche Situation in geeigneter Form zu verdeutlichen. Hiervon habe ich auch den zuständigen Landesminister unterrichtet.

Gegen die Verquickung von Statistik und Verwaltungsvollzug bestehen aber auch grundsätzliche Bedenken. Das Vertrauen der Bevölkerung auf die Integrität der statistischen Geheimhaltung beruht wesentlich auf der Gewißheit, daß der statistische Informationsfluß von den Aufgaben des Verwaltungsvollzuges strikt getrennt ist. Jede Ausnahme von diesem Prinzip ist — gleichviel um welche Daten und um welche administrative Verwendung es geht — bereits deshalb gefährlich, weil sie die Situation unübersichtlich macht, die Bürger verunsichert und dadurch das „statistische Klima" empfindlich stören kann.

Der Trennungsgrundsatz hat aber auch eine verfassungsrechtliche Wurzel. Die Verpflichtung zur Offenlegung persönlicher Angelegenheit ist nach der Auffassung des Bundesverfassungsgerichts in bestimmten Grenzen mit dem Grundgesetz im Hinblick darauf vereinbar, daß „diese Angaben durch die Anonymität ihrer Auswertung den Persönlichkeitsbezug verlieren" (BVerfGE 27, 7).

Die unbestreitbaren wirtschaftlichen Vorteile der Verbunderhebung dürften die Nachteile und Bedenken kaum aufwiegen. Rationelle Erhebungsverfahren ließen sich im übrigen auch auf anderem Wege erreichen, etwa dadurch, daß dem Betroffenen ein Computerausdruck aus der Verwaltungsdatei ausgehändigt wird, der von ihm um statistische Angaben zu erweitern und dann dem statistischen Amt zu übersenden ist.

Ich empfehle deshalb, in der künftigen statistischen Fachgesetzgebung eine administrative Nutzung statistischer Daten nicht mehr zuzulassen und die Regelungen des Hochschulstatistikgesetzes mit dem Ziel zu überprüfen, das Trennungsprinzip auch hier zu realisieren.

3.3.4 Mikrozensus

Der „Mikrozensus", eine auf gesetzlicher Grundlage erhobene Bundesstatistik (Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens vom 15. Juli 1975, BGBl. I S. 1909) war Gegenstand mehrerer Beschwerden betroffener Bürger. Auch Abgeordnete des Deutschen Bundestages haben mir von Unmutsäußerungen und Protesten in der Bevölkerung berichtet. Die Beschwerden richten sich gegen die Fragen, die am tiefsten in den persönlichen Bereich eingreifen, z. B. über Rauchgewohnheiten und Erkrankungen. Die Beantwortung solcher Fragen halten viele Bürger jedenfalls solange für unzumutbar, wie die Daten unter Angabe ihres Namens und ihrer Anschrift erhoben und aufbewahrt werden.

Ich konnte in solchen Fällen den Bürgern nur mitteilen, daß sie nach dem Bundesstatistikgesetz auskunftspflichtig seien und daß das Mikrozensusgesetz auch „Fragen zur Gesundheit" zulasse. Außerdem habe ich darauf hingewiesen, daß alle persönlichen Angaben dem — strafrechtlich abgesicherten — Statistikgeheimnis unterliegen und daß mir bisher noch kein Fall einer Verletzung der statistischen Geheimhaltung bekanntgeworden ist.

Für unproblematisch halte ich die Befragung gleichwohl nicht. Nach der Rechtsprechung des Bundesverfassungsgerichts zu den Grundrechten aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG muß der Bür-

ger statistische Erhebungen als Ausdruck seiner Sozialgebundenheit zwar in gewissem Umfange hinnehmen, z. B. dann, wenn eine Erhebung „nur an das Verhalten des Menschen in der Außenwelt anknüpft" und „diese Angaben durch die Anonymität ihrer Auswertung den Persönlichkeitsbezug verlieren". Demgegenüber steht jedoch der „Bereich menschlichen Eigenlebens, der von Natur aus Geheimnischarakter hat" (BVerfGE 27, 7).

Ohne damit eine verfassungsrechtliche Würdigung zu verbinden, ist festzustellen, daß es sich bei Fragen nach Krankheiten und Unfallverletzungen sowie nach der Höhe des gegenwärtigen oder früheren Tabakkonsums um Tatbestände handelt, die zwar in manchen Fällen zum „Verhalten in der Außenwelt" gehören, vielfach aber allein dem Auskunftspflichtigen bekannt sind. Genau dies ist nach meinen Wahrnehmungen auch der Grund dafür, daß viele Bürger das Auskunftsverlangen als einen Einbruch in ihren privatesten Bereich betrachten, der sich mit ihrer Vorstellung vom Verhältnis zwischen Bürger und Staat nicht vereinbaren läßt. Die Belastungen, die sich hieraus ergeben, betrachte ich mit Sorge.

Aus diesen Gründen habe ich angeregt, zu überprüfen, ob sich im Rahmen der laufenden Gesetzgebungsvorhaben auf dem Gebiet der Bundesstatistik eine Möglichkeit ergibt, von einer Auskunftspflicht bezüglich der Fragen zur Gesundheit für die Zukunft abzusehen. Gegen eine freiwillige Erhebung, die nach § 7 Abs. 2 des Bundesstatistikgesetzes entsprechend zu kennzeichnen wäre, hätten die Betroffenen nach meinen Erfahrungen wenig einzuwenden, insbesondere dann, wenn sie über Sinn und Zweck einer solchen Befragung hinreichend aufgeklärt werden und für die Anonymisierung Sorge getragen ist. Der Bundesminister des Innern hat angekündigt, daß sich die Bundesregierung in der Gegenäußerung zur Stellungnahme des Bundesrates zum Entwurf eines Statistikbereinigungsgesetzes für eine freiwillige Erhebung aussprechen werde.

3.3.5 Entwurf für ein Volkszählungsgesetz 1981; Novellierung des Bundesstatistikgesetzes

Im Rahmen meiner beratenden Tätigkeit habe ich zu dem vom Bundesminister des Innern vorgelegten Gesetzentwurf über eine Volks-, Berufs- und Arbeitsstättenzählung (Volkszählungsgesetz 1981, BR-Drucksache 444/78) Stellung genommen. Ich habe mich dabei von folgenden Grundsätzen leiten lassen:

— Das Gesetz soll möglichst eng präzise umschreiben, in welchem Umfang der einzelne Bürger verpflichtet ist, Angaben für die Statistik zu machen.

— Die vom Bürger gemachten Einzelangaben dürfen nur für statistische Zwecke, nicht aber für Entscheidungen oder Maßnahmen in bezug auf die einzelne auskunftgebende Person verwendet werden.

— Dies gilt auch bei der Übermittlung von Einzelangaben: sie dürfen dem Empfänger nur als „Rohstoff" zur Gewinnung von Informationsgrundlagen für Planung und Wissenschaft überlassen werden. Vorsorge gegen Mißbrauch ist notwendig.

— Dem Betroffenen soll verdeutlicht werden, daß seine Angaben der Geheimhaltung unterliegen, ggf. aber auch, in welchen Fällen ausnahmsweise eine Übermittlung zulässig ist.

Ein wesentlicher Teil meiner Anregungen ist in den Regierungsentwürfen des Volkszählungsgesetzes und des Bundesstatistikgesetzes (BR-Drucksache 443/78) berücksichtigt worden. So wurde beispielsweise auf Grund meines Hinweises auf Artikel 4 GG in Verbindung mit Artikel 136 Abs. 3 Weimarer Verfassung, wonach grundsätzlich niemand verpflichtet ist, seine religiöse Überzeugung zu offenbaren — ausgenommen für gesetzlich angeordnete statistische Erhebungen — besonders festgelegt, daß die Angabe über die Religionszugehörigkeit von der Übermittlung an andere Stellen ausgeschlossen bleibt. Das Risiko einer nicht-statistischen Verwendung durch einen Empfänger ist damit beseitigt. Weiter wurde klargestellt, daß Einzelangaben vom Empfänger jeweils nur für den Zweck verwendet werden dürfen, für den sie ihm übermittelt wurden, also z. B. für eine bestimmte wissenschaftliche Untersuchung oder eine bestimmte Planungsaufgabe (vgl. § 9 Abs. 5 des Entwurfs eines Volkszählungsgesetzes). Ich betrachte damit *jede* auf die Einzelperson bezogene Verwendung als ausgeschlossen. Die Verweisung auf die schwächere Regelung des § 9 Abs. 1 Satz 2, der lediglich „Maßnahmen *gegen* den einzelnen Auskunftspflichtigen" verbietet, ist daher überflüssig. Aus ihr kann jedenfalls kein Umkehrschluß gezogen werden. Da der Grundsatz der Zweckbindung von allgemeiner Bedeutung ist, sollte er auch im Bundesstatistikgesetz seinen Ausdruck finden. Meine Empfehlung, die Auskunftspflichtigen durch entsprechende Aufdrucke auf den Erhebungsbogen über die gesetzlich zugelassenen Fälle der Datenübermittlung umfassend aufzuklären, hat die Bundesregierung bereits entsprechend berücksichtigt (vgl. § 11 Abs. 3 des Entwurfs eines Bundesstatistikgesetzes).

In verschiedenen anderen Punkten wurde jedoch noch keine aus der Sicht der einzelnen Betroffenen befriedigende Lösung gefunden. Dies sei an drei Beispielen aufgezeigt.

— Nach dem Entwurf ist jede volljährige sowie jede minderjährige Person, die einen eigenen Haushalt führt, auskunftspflichtig. Zusätzlich gibt es die sog. Ersatzauskunftspflicht: die genannten Personen sind auch für minderjährige oder behinderte Haushaltsmitglieder auskunftspflichtig; für Personen in Gemeinschaftsunterkünften, Anstalten und ähnlichen Einrichtungen müssen auch deren Leiter Auskünfte geben (§ 5 des Entwurfs).

  Diese Regelung stößt zunächst deshalb auf Bedenken, weil sie die Inanspruchnahme von Ersatzauskunftspflichtigen nicht auf die Fälle beschränkt, in denen dies sachlich geboten ist. Deshalb ist damit zu rechnen, daß sich die mit der Erhebung betrauten Personen schon aus arbeitsökonomischen Gründen bevorzugt an die Anstaltsleitungen und sog. Haushaltsvorstände wenden. Für die Betroffenen ist dieses Verfahren je-

doch mit einer zusätzlichen Gefährdung ihres Datenschutzes verbunden. Da das Gesetz auch vom Ersatzauskunftspflichtigen uneingeschränkt wahrheitsgemäße und vollständige Angaben verlangt, kann nicht ausgeschlossen werden, daß dieser den Betroffenen die Informationen abfordert, die er aus eigenem Wissen nicht beantworten kann. Nicht jeder Bewohner eines Alters- oder Studentenheimes wird es aber begrüßen, wenn die Heimleitung sich auf diesem Wege Informationen über die Quellen seines Lebensunterhalts oder über seine Religionszugehörigkeit verschafft. Bei der Auskunftspflicht von volljährigen über minderjährige Haushaltsmitglieder wären zudem die Regelungen über die Religionsmündigkeit nach dem Gesetz über die religiöse Kindererziehung zu beachten.

Hinzu kommt, daß die Ersatzauskunftspflichtigen nicht dem Statistikgeheimnis und den entsprechenden Strafvorschriften unterliegen, da sie nicht Auskunftsberechtigte im Sinne des § 12 Abs. 1 Bundesstatistikgesetz, sondern Auskunftsverpflichtete sind.

Ich rege daher an, die Ersatzauskunftspflicht auf diejenigen Fälle zu beschränken, in denen der Betroffene zur Auskunftserteilung nicht in der Lage ist (etwa aus Altersgründen oder wegen geistiger Behinderung), und darüber hinaus ausdrücklich festzulegen, daß der Ersatzauskunftspflichtige Angaben nur aus dem vorhandenen Wissen zu machen hat, zu ergänzenden Ermittlungen jedoch weder verpflichtet noch berechtigt ist.

— Problematisch ist auch die vorgesehene Regelung des sog. Abgleichs mit den Melderegistern der Gemeinden (§ 9 Abs. 1). Die Vorschrift erlaubt es den Gemeinden, die Angaben der Bürger über Vor- und Familiennamen, Geburtsdatum, Familienstand und Anschriften mit ihren Verwaltungsunterlagen zu vergleichen und gegebenenfalls zur Berichtigung zu verwenden. Zwar geht es hier nur um wenige Grunddaten. Auch verbietet das Gesetz ausdrücklich, die solcherart gewonnenen Erkenntnisse zu „Maßnahmen gegen den einzelnen Auskunftspflichtigen" zu verwenden. Dennoch bestehen grundsätzliche Bedenken, weil es sich auch hier um eine Durchbrechung des Prinzips der strikten Trennung von Statistik- und Verwaltungsvollzug handelt (vgl. dazu näher oben 3.3.3), die durch die bezweckte administrative Erleichterung nicht gerechtfertigt wird.

— Die strafrechtliche Absicherung des Statistikgeheimnisses weist noch weitere Lücken auf. Es fehlen Sanktionsmöglichkeiten für den Fall, daß sich jemand durch falsche Angaben den Zugang zu Einzelangaben erschleicht, wie es z. B. beim „Stuttgarter Datenskandal" (vgl. die Entscheidung des Landgerichts Bad Kreuznach, Neue Juristische Wochenschrift 1978, S. 1931) der Fall gewesen ist.

Die §§ 203 und 204 des Strafgesetzbuchs decken nur einen Teil der hier in Betracht kommenden Fälle ab. In diesem Zusammenhang sollte auch der Fall miterfaßt werden, daß derjenige, der Einzelangaben ohne Namen zur statistischen, insbesondere planerischen oder wissenschaftlichen — also nicht personenbezogenen — Auswertung erhalten hat, versucht, den Bezug zu bestimmten Personen wieder herzustellen (Rückidentifikation).

3.3.6 Wissenschaftliche Forschung und Statistikgeheimnis

3.3.6.1 Enzelangaben und Anonymisierung

Von einem wissenschaftlichen Institut ist darüber Klage geführt worden, daß das Statistische Bundesamt ihm nicht mehr die für seine Arbeit unerläßlichen Daten zur Verfügung stelle, obwohl aus dem erbetenen Material keinerlei Rückschlüsse auf bestimmte Personen möglich seien. Die Meinungsverschiedenheit liegt im Wortlaut der Vorschrift über das Statistikgeheimnis begründet. § 12 Abs. 1 Bundesstatistikgesetz verlangt, „Einzelangaben über persönliche oder sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, ... geheim zu halten". In Absatz 3 heißt es weiter: „Eine Zusammenfassung von Angaben mehrerer Auskunftspflichtiger ist keine Einzelangabe im Sinne dieses Gesetzes". Daraus könnte abgeleitet werden, daß es sich bei nicht-aggregierten Daten (Mikrodaten) stets um geheimzuhaltende Einzelangaben im Sinne des Gesetzes handelt, ohne Rücksicht darauf, ob die Person oder Stelle, auf die sich die Daten beziehen (oder bezogen haben), erkennbar ist.

Ich teile diese Auffassung nicht. Das Kriterium des BDSG, das auf die Bestimmbarkeit des Betroffenen abstellt, grenzt die Belange des Informationsbetroffenen und des Informationsinteressenten überzeugender ab: Die Rechte des Betroffenen können der Übermittlung nur solange entgegenstehen, wie es sich um eine gerade auf ihn bezogene oder beziehbare Information handelt. Meines Erachtens kann diese Begrenzung auch unmittelbar aus dem Schutzzweck des Statistikgeheimnisses entnommen werden. Im übrigen betrachte ich es als eine Belastung des Gedankens des Datenschutzes, wenn die Verweigerung von Daten auf Datenschutzgründe gestützt wird, ohne daß tatsächlich irgendeine Person oder Stelle in ihren Rechten verletzt wird.

Ich begrüße es deshalb, daß die Bundesregierung in der Begründung zu § 11 Abs. 1 des Entwurfs eines Bundesstatistikgesetzes (BR-Drucksache 443/78) klargestellt hat, daß einwandfrei anonymisierte Einzelangaben nicht geheimgehalten zu werden brauchen.

3.3.6.2 Angaben öffentlicher Stellen

Von Wissenschaftlern wurde ferner kritisiert, daß ihnen der Zugang zu Daten verweigert wurde, die sich nicht auf Personen oder Unternehmen beziehen, sondern auf Behörden oder Gebietskörperschaften. Die statistischen Ämter vollziehen insoweit jedoch lediglich die in § 12 Bundesstatistikgesetz vorgesehene Regelung. Zu schützen ist danach jede Auskunftspflichtige, gleichgültig ob es sich um

eine Privatperson oder ein Subjekt des öffentlichen Rechts handelt. Sachlich überzeugend ist diese pauschale Gleichstellung jedoch nicht. Bei Angaben, die sich auf juristische Personen des öffentlichen Rechts, insbesondere auf Gebietskörperschaften, beziehen, fehlt es vielfach an einem Geheimhaltungsbedürfnis. Es ist nicht nur unschädlich, sondern durchaus wünschenswert, wenn die mit hohem Aufwand an öffentlichen Mitteln erhobenen Angaben in möglichst großem Umfang auch Außenstehenden für eigene Auswertungen zur Verfügung stehen. Ich rege deshalb an, künftig bei der Vorbereitung statistischer Einzelgesetze in den Fällen, in denen öffentliche Stellen zur Auskunft verpflichtet sind, jeweils besonders zu überprüfen, ob die Angaben vom Statistikgeheimnis ausgenommen werden können.

3.3.6.3 Übermittlungsregelung im Entwurf eines Bundesstatistikgesetzes

Im Hinblick auf eine möglichst gute Zugänglichkeit solcher Daten, die voll wirksam anonymisiert sind und daher die Rechte von Personen oder Institutionen nicht tangieren können, erscheint mir die in § 11 Abs. 3 des Entwurfs eines Bundesstatistikgesetzes vorgesehene abschließende Regelung für die Übermittlung von Einzelangaben — mit Wirkung auch für künftige statistische Einzelgesetze — nicht unbedenklich. Abgesehen von den obersten Bundes- und Landesbehörden und den von ihnen bestimmten Stellen werden dort als mögliche Empfänger lediglich die „sonstigen Amtsträger und für den öffentlichen Dienst besonders Verpflichteten" vorgesehen. Aus der Begründung des Entwurfs ergibt sich, daß die Grenze so gezogen wurde, daß die Empfänger im Falle eines Mißbrauchs nach den §§ 203, 204 StGB (Verletztung von Privatgeheimnissen) belangt werden können. Gewiß ist es notwendig, daß im Falle eines Mißbrauchs durch die Empfänger statistischer Einzelangaben eine Sanktionsmöglichkeit besteht. Ich hielte es jedoch für folgerichtiger, die Strafvorschriften an den statistischen Übermittlungsvorschriften auszurichten, als umgekehrt. Bei der Fassung des Regierungsentwurfs bestehen Zweifel, ob ein Hochschulinstitut, sofern es nicht ausnahmsweise in behördlichem Auftrag arbeitet, in Zukunft noch statistische Einzelangaben erhalten könnte. So sehr es mir darauf ankommt, das Statistikgeheimnis zu sichern, so wenig würde ich es doch für angemessen halten, die unabhängig betriebene Hochschulforschung vom Zugang zu statistischen Einzelangaben (wozu wegen der Rückiddentifizierbarkeit auch Daten ohne Namen und Anschrift gehören können) generell auszuschließen.

3.4 Öffentliche Sicherheit und Ordnung, Verteidigung

3.4.1 Anwendbarkeit des Bundesdatenschutzgesetzes

Entgegen einem verbreiteten Irrtum gelten für die Sicherheitsbehörden des Bundes, nämlich das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), den Bundesnachrichtendienst (BND) und den militärischen Abschirmdienst (MAD) sowie das Wehrersatzwesen die materiellen Regelungen des BDSG über die Zulässigkeit der Speicherung, Übermittlung, Veränderung und Löschung von personenbezogenen Daten grundsätzlich ebenso wie für andere öffentliche Stellen des Bundes; außerdem gilt selbstverständlich das bisher vorhandene bereichsspezifische Datenschutzrecht. Allerdings hat der Gesetzgeber aus Sicherheitsgründen Ausnahmen im Gesetz vorgesehen: Nach § 12 Abs. 2 Nr. 1 BDSG sind die angeführten Sicherheitsbehörden (und einige weitere Behörden) nicht zur Veröffentlichung der von ihnen geführten Dateien verpflichtet, und nach § 13 Abs. 2 brauchen sie den Betroffenen keine Auskunft über die gespeicherten Daten zu erteilen. Wie noch im einzelnen zu zeigen ist, werden diese Nachteile für die Betroffenen teilweise dadurch ausgeglichen, daß die genannten Behörden meiner Kontrolle unterliegen. Trotz praktischer Schwierigkeiten haben die bisherigen Kontakte mit den Sicherheitsbehörden des Bundes zu Fortschritten bei der Verwirklichung von Datenschutz auch in diesem Bereich geführt.

3.4.2 Art und Umfang der Kontrolle

Ich betrachte die datenschutzrechtliche Kontrolle der Sicherheitsbehörden als eine Schwerpunktaufgabe meines Amtes. Diese Behörden verarbeiten besonders empfindliche und weit in die Privatsphäre hineinreichende Daten, und zwar im wesentlichen ohne Kontrollmöglichkeit der Betroffenen. Die Ombudsman-Funktion nach § 21 BDSG hat in diesem Bereich besondere Bedeutung.

Zwar sind auch meine Kontrollbefugnisse nach § 19 Abs. 3 Satz 4 BDSG ausgeschlossen, soweit „die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet". Dieser Vorbehalt wird aber nach meiner Einschätzung kaum je aktuell werden. Selbstverständlich wahre ich die gesetzliche Verschwiegenheitspflicht; auch soweit Betroffene mich um Prüfungen in ihrem Interesse bitten, fühle ich mich durch das Geheimhaltungsgebot gebunden, solange nicht die speichernde Stelle selbst die betreffende Information freigibt. Nach Durchführung von Kontrollen kann daher nur das Ergebnis der rechtlichen Bewertung mitgeteilt werden (im einzelnen vgl. unten 3.4.7.3). Daß die Durchführung meiner Kontrolltätigkeit im Einzelfall auf Sicherheitsbedenken stoßen könnte, ist nur in Extremfällen vorstellbar.

Die praktischen Schwierigkeiten bei der Ausübung des Kontrollrechts werden im folgenden Abschnitt exemplarisch für das Bundesamt für Verfassungsschutz behandelt.

3.4.3 Bundesamt für Verfassungsschutz

3.4.3.1 Der Auftrag des BfV

Das BfV hat den gesetzlichen Auftrag, Unterlagen über Bestrebungen gegen die freiheitliche demokra-

tische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland und über geheimdienstliche Tätigkeiten zu sammeln und auszuwerten (vgl. im einzelnen § 3 des Gesetzes über die Zusammenarbeit des Bundes und der Länder auf dem Gebiet des Verfassungsschutzes, eine Vorschrift, die als bereichsspezifische Regelung des Datenschutzes nach § 45 BDSG dessen Bestimmungen vorgeht, soweit in Dateien gespeicherte personenbezogene Daten betroffen sind). Damit obliegt ihm eine Art von Informationsverarbeitung, die für den Datenschutz besondere Probleme aufwirft. „Bestrebungen" im Sinne des Verfassungsschutzgesetzes können hinter unzähligen „harmlosen" sozialen Verhaltensweisen wie dem Besuch beliebiger Versammlungen und Reisen zu beliebigen Zielen vermutet werden; Information über solche nicht nur rechtmäßigen, sondern sogar grundrechtlich geschützten Handlungsweisen können also für Verfassungsschutzbehörden zumindest theoretisch ebenso interessant sein wie die Nachricht über ein konspiratives Treffen zweier ausländischer Spione. Die Ämter für Verfassungsschutz sollen nicht nur die Regierungen laufend allgemein über Vorgänge informieren, die um der Sicherheit des Staates und der Freiheitlichkeit der politischen Entwicklung willen die Aufmerksamkeit der politischen Führung verdienen, sondern auch Material für eventuell in der Zukunft einzuleitende Maßnahmen gegen einzelne Bürger vorbereiten. Sie arbeiten im *Vorfeld* staatlicher Reaktionen auf ein rechtlich mißbilligtes Verhalten und in einem Feld, auf dem die Einleitung von staatlichen Maßnahmen zu einem nicht unbeträchtlichen Teil von politischen Opportunitätserwägungen abhängt. Soweit die Verfassungsschutzbehörden Informationen über einzelne Personen speichern, tun sie dies zur Vorbereitung auf einen möglicherweise nie eintretenden Fall. Denn bevor solche Informationen in konkrete Verwaltungstätigkeit, z. B. polizeiliche Maßnahmen der Gefahrenabwehr oder die Einleitung eines Strafverfahrens, umgesetzt werden, muß eine gewisse Relevanzschwelle überschritten werden. In anderen Fällen geschieht eine personenbezogene Auswertung gesammelten Materials erst aus besonderem Anlaß, z. B. — um einen besonders akutellen Fall zu nennen — dem einer Bewerbung um Einstellung in den öffentlichen Dienst. Vielfach aber kommt es gar nicht zu irgendwelchen erkennbaren staatlichen Reaktionen auf die zur Kenntnis genommenen Sachverhalte, jedenfalls nicht gegen einzelne Personen (z. B. wenn nur die Absichten bestimmter Organisationen bekanntgemacht werden); häufig dürfte auch fraglich sein, ob Sanktionen überhaupt zulässig wären (weil nämlich die beobachtete Handlung nicht verboten war).

Wenn die Verfassungsschutzämter ihren gesetzlichen Auftrag ausführen, stoßen sie wegen der geschilderten Besonderheiten notwendigerweise auf entgegengesetzte Freiheitsansprüche der betroffenen Bürger. Staatliches Informationsinteresse, wie es im Verfassungsschutzgesetz seine Anerkennung findet, und die schützenswerten Interessen des einzelnen, die unter anderem durch das Datenschutzrecht gewährleistet werden sollen, stehen hier in einem unausweichlichen Zielkonflikt. Dieser Zielkonflikt kann nicht dadurch überwunden werden, daß der eine Gesichtspunkt völlig hinter dem anderen zurücktritt. Auch die Verfassung enthält hier keine klare Aussage. Das Grundgesetz gestattet in Artikel 87 Abs. 1 Satz 2 die Einrichtung von „Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei und zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes" usw. Andererseits finden die Rechte der Betroffenen eine starke Stütze in den Grundrechtsnormen des Grundgesetzes, insbesondere Artikel 1 Abs. 1, Artikel 2 Abs. 1, Artikel 4 Abs. 1 und Artikel 5 Abs. 1

Es muß eine Lösung des Ziel- und Normenkonflikts gesucht werden, die den *beiden* vom Gesetzgeber und von der Verfassung anerkannten Zielen möglichst weit gerecht wird. Hierzu sind differenzierende Überlegungen erforderlich.

Die Tätigkeit der Verfassungsschutzbehörden ist um so weniger problematisch, je mehr sie sich darauf konzentriert, der Regierung Lageberichte allgemeiner Art zu liefern. Sie ist um so kritischer zu betrachten, je weiter ins Vorfeld möglicher Maßnahmen die Sammlung personenbezogener Daten über einzelne Bürger ausgedehnt wird. Eine solche Praxis kann leicht mit einem wesentlichen Prinzip richtig verstandenen Datenschutzes kollidieren, das häufig übersehen wird, nämlich dem Gebot, Daten nur für konkrete Verwaltungs- und Geschäftszwecke zu sammeln, insbesondere (im öffentlichen Bereich) zur Vorbereitung bestimmter oder doch bereits in Umrissen bestimmbarer Verwaltungsakte, anders ausgedrückt, dem Verbot der Sammlung von Daten auf Vorrat, ohne besonderen Anlaß. Dieses Prinzip hat als solches zwar keinen Verfassungsrang, kann aber im Einzelfall aus einem Grundrecht des Betroffenen folgen.

Die weite und generalklauselartige, vielfältig interpretierbare Aufgabenbestimmung des Verfassungsschutzgesetzes sowie die Tatsache, daß diese Aufgaben durch geheime nachrichtendienstliche Tätigkeit erfüllt werden muß, sind wesentliche Quellen der verbreiteten Unruhe und des Mißtrauens gegenüber den Ämtern für Verfassungsschutz. Wenn eine offen arbeitende Behörde der Öffentlichkeit auffällt, z. B. durch eine für rechtswidrig gehaltene Maßnahme, beschränkt sich die Diskussion in aller Regel auf den jeweiligen Einzelfall; wenn eine geheim arbeitende Behörde mit extensivem Informationsauftrag auffällig und möglicherweise rechtswidrig handelt, entsteht bei den Bürgern sogleich die Besorgnis, daß sie es generell mit der Bindung an Verfassung und Gesetz nicht ernst genug nehme. Die Nachrichtendienste des Bundes sind sich nach meinem Eindruck darüber im klaren, daß dieses Mißtrauen besteht und daß es nur abgebaut werden kann, wenn die eigene Praxis strengen rechtsstaatlichen Maßstäben genügt. Ich habe auch keine Anhaltspunkte dafür gefunden, daß die geltenden Rechts- und Verwaltungsvorschriften, welche die Tätigkeit dieser Behörden ordnen und einschränken, mißachtet würden. Allerdings folgt aus der dargestellten Situation, daß über weitere rechtliche Regelungen nachgedacht werden muß, welche die Tätigkeit der Verfassungsschutzbehörden (wie auch der übrigen Nachrichtendienste) verfassungskonform

ordnen. Mit den oben angeführten Aufgabennormen des Verfassungsschutzgesetzes ist zwar ein Anfang gemacht, und ergänzend gilt das BDSG. Doch sind diese Normen weiter zu konkretisieren.

Soweit Informationen in Dateien verarbeitet oder aus Dateien übermittelt werden, sind die materiellen Bestimmungen des BDSG zu beachten, voran §§ 9 bis 11, in denen der Erforderlichkeitsgrundsatz betont ist. Dieser ist verfassungsrechtlich fundiert; er folgt aus dem Prinzip der Verhältnismäßigkeit, das seinerseits aus dem Rechtsstaatsprinzip hergeleitet ist. Nur dasjenige Material darf also gesammelt und gespeichert werden, das für die Erfüllung des — freilich, wie ausgeführt, sehr weiten — Auftrages der Behörden für Verfassungsschutz unumgänglich notwendig ist. Das Bundesverfassungsgericht hat dies im „Abhör-Urteil" für den Anwendungsbereich des Gesetzes zu Artikel 10 GG ausgeführt (BVerfGE 30, 1, 21/22). Danach dürfen nur Personen überwacht werden, die in einen konkreten Verdacht der im Gesetz beschriebenen Art geraten sind; die Überwachung darf „auf nichts anderes gerichtet" sein „als auf die Erlangung der Kenntnis von verfassungsfeindlichen Vorgängen" (BVerfG a. a. O. S. 22). Zum Abhörgesetz hat das BVerfG auch ein verfassungsrechtliches Verbot festgestellt, „die durch die Überwachung erlangte Kenntnis anderen (Verwaltungs-) Behörden für ihre Zwecke" zugänglich zu machen, und ein Gebot, „anfallendes Material, das nicht oder nicht mehr für die Zwecke des Schutzes der freiheitlichen demokratischen Ordnung bedeutsam ist, unverzüglich" zu vernichten (a. a. O. S. 22/23, vgl. auch § 3 Abs. 2 und § 7 Abs. 3 G 10).

Bei der Übertragung solcher Rechtsgrundsätze auf die Behörden für Verfassungsschutz ist zu beachten, daß ihnen — von der Sicherheitsüberprüfung nach § 3 Abs. 2 des Verfassungsschutzgesetzes abgesehen — nicht die Überwachung von Personen, sondern — wie ausgeführt — von „Bestrebungen" obliegt. Personen können in diesem Zusammenhang als „Träger von Bestrebungen" in Erscheinung treten, darüber hinaus können auch Nachrichten über Einzelpersonen gesammelt werden, die Verbindungen zu Trägern verfassungsfeindlicher Bestrebungen unterhalten, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß die Beobachtung zu wesentlichen Erkenntnissen für die Aufgaben des Verfassungsschutzes führen kann (vgl. Evers, Privatsphäre und Ämter für Verfassungsschutz, 1960, S. 124; Rottmann, Archiv für öffentliches Recht Band 88 S. 233). In jedem Fall muß darauf geachtet werden, daß die betroffenen Personen nicht mit strafrechtlich Angeschuldigten gleichgesetzt werden dürfen; wenn sie als „Verdächtige" bezeichnet werden, ist immer die besondere Bedeutung zu beachten, die sich aus der Aufgabe des Verfassungsschutzes ergibt.

Aus der Verfassung und den Gesetzen ableitbare rechtliche Einschränkungen sind auch in interne Vorschriften des Bundesamtes für Verfassungsschutz umgesetzt worden. So ist es den Mitarbeitern dieses Amtes beispielsweise keineswegs gestattet, beliebige Organisationen, Objekte oder Personen zu beobachten. Die Entscheidung darüber, welche Objekte zu beobachten sind, obliegt dem Präsidenten des Amtes. Vereinigungen, bei denen nach ihrem bisherigen Verhalten und nach dem sie tragenden Personenkreis feststeht, daß sie auf dem Boden der freiheitlichen demokratischen Grundordnung stehen, dürfen mit Mitteln der Nachrichtenbeschaffung, insbesondere durch geheime Mitarbeiter, nicht beobachtet werden (§ 11 der Dienstanweisung für das BfV). Jede Beobachtung verfassungsfeindlicher Bestrebungen hat sich streng an den Beobachtungszweck zu halten. Jede Ausweitung ist unzulässig.

Ehe die gesammelten Informationen in die Akten gelangen, werden sie gefiltert. Fachkräfte, die mit dem Ermittlungspersonal nicht identisch sind, haben nach Maßgabe einer „Dienstvorschrift für die Auswertung" zu prüfen, ob das Material für die Erfüllung der gesetzlichen Aufgaben erforderlich ist. Ein Teil wird bereits in diesem Stadium als nicht relevant ausgeschieden und vernichtet. Nach § 7 Abs. 2 der Dienstanweisung und nach Nummer 7 der Dienstvorschrift für die Auswertung sind darüber hinaus Unterlagen, die die Privatsphäre einer Person betreffen, unverzüglich zu vernichten, soweit sie nicht für Angelegenheiten des Verfassungsschutzes notwendig sind. Diese Konkretisierungen des verfassungsrechtlichen Erforderlichkeitsprinzips können — zumindest als Ausgangspunkt — auch als Maßstab meiner Kontrolltätigkeit dienen. Für Erkenntnisse, die durch Abhörmaßnahmen nach dem Gesetz zu Artikel 10 GG gewonnen sind, folgen diese Gebote schon unmittelbar aus dem Gesetz. § 7 Abs. 4 G 10 verlangt nämlich die Vernichtung allen nicht mehr erforderlichen Materials. Die Vernichtung muß unter Aufsicht geschehen; es ist eine Niederschrift darüber anzufertigen. Dies gilt im übrigen auch für die beiden anderen Nachrichtendienste, die befugt sind, im Rahmen des Gesetzes zu Artikel 10 GG zu handeln (BND und MAD).

Die Schwelle, oberhalb deren die Tätigkeit des Verfassungsschutzes einzusetzen hat, bei der also Material zu speichern ist, kann im voraus nicht hinreichend eindeutig abgegrenzt werden. Daher wird es auch künftig unvermeidbar sein, daß das BfV seine Aufmerksamkeit Personen widmet, bei denen sich nach einer gewissen Zeit zweifelsfrei ergibt, daß sie keine verfassungsfeindlichen Bestrebungen verfolgen.

Hier besteht eine Rechtspflicht, die entsprechenden Unterlagen in diesem Zeitpunkt von Amts wegen zu löschen.

3.4.3.2 Übermittlung von Daten durch das BfV

Werden personenbezogene Daten aus dem Bereich des Verfassungsschutzes an Dritte übermittelt, so stellt dieser Vorgang einen weitaus intensiveren und nachhaltigeren Eingriff in die Rechtssphäre des Betroffenen dar, als es bei der Sammlung und Speicherung der Fall ist, zumal es sich ja um Daten handelt, die überwiegend ohne Wissen und Zutun des Betroffenen ermittelt und gespeichert worden sind und daher von ihm nicht auf ihre Richtigkeit überprüft werden konnten. Das BfV darf die Daten nicht etwa mehr oder weniger wahllos weitergeben. Zunächst verlangt schon die vom Bundesinnenminister erlas-

sene „Dienstvorschrift für die Auswertung", daß an die Richtigkeit und Zuverlässigkeit der ermittelten Erkenntnisse hohe Anforderungen zu stellen und daß bestehende Zweifel zum Ausdruck zu bringen sind. Anderen Stellen als Verfassungsschutzbehörden oder Nachrichtendiensten sollen in der Regel nur Erkenntnisse mitgeteilt werden, die als gesichert angesehen werden können. Wird es im Einzelfall für erforderlich gehalten, auch nicht gesicherte Erkenntnisse zu übermitteln, so sind die Zweifel an der Richtigkeit zum Ausdruck zu bringen. Bei Übermittlung von Daten an ausländische Nachrichtendienste ist das BfV nach § 18 Abs. 3 der Dienstanweisung ausdrücklich gehalten, diesen gegenüber die staatsbürgerlichen Rechte von Deutschen zu wahren.

Diese Differenzierungen sind jedoch noch nicht ausreichend. Vielmehr ist gerade in dem Aufgabenbereich des BfV sicherzustellen, daß die Weitergabe von Erkenntnissen an andere Behörden besonders restriktiv gehandhabt wird. Hier kann deshalb auch nicht der weite Rahmen von § 10 BDSG gelten, wonach eine Übermittlung bereits dann zulässig ist, wenn die Erkenntnisse für die rechtmäßige Erfüllung der Aufgaben des Empfängers erforderlich sind. Diese Bestimmung kann allein für den Datenverbund innerhalb der Nachrichtendienste selbst Relevanz beanspruchen. Eine Übermittlung von Daten aus dem Bereich des Verfassungsschutzes an andere Stellen als Nachrichtendienste darf dagegen nur dann erfolgen, wenn dies zur Erfüllung von Aufgaben notwendig ist, die dem BfV bzw. den Verfassungsschutzbehörden zugewiesen sind. Als Beispiel sei die Strafverfolgung von Staatsschutzdelikten genannt. Für die Durchführung entsprechender Ermittlungsverfahren dürfen den Strafverfolgungsbehörden einschlägige Erkenntnisse des Verfassungsschutzes mitgeteilt werden. Für die Verfolgung anderer Delikte dagegen, wie z. B. von Eigentums- oder Steuervergehen, darf das BfV auch gesicherte Erkenntnisse nicht übermitteln, denn das widerspräche der grundsätzlichen Aufgaben- und Befugnistrennung der staatlichen Stellen untereinander, die durch die allgemeine Pflicht zur Amtshilfe nicht aufgehoben werden kann. Diese Einschränkung entspricht auch der in § 3 Abs. 2 und § 7 Abs. 3 G 10 bestimmten engen Begrenzung für die Weitergabe von Informationen, die durch Maßnahmen nach jenem Gesetz gewonnen werden. Der Gedanke der Einheit der Staatsgewalt kann hiergegen auch deshalb nicht ins Feld geführt werden, weil spätestens seit der Verabschiedung des BDSG feststeht, daß der Gewaltenteilung in bezug auf Entscheidungskompetenzen eine rechtlich geordnete Verteilung der Informationsmengen auf verschiedene Stellen der staatlichen Organisation entspricht.

Eine entsprechende gesetzliche Klarstellung wäre wünschenswert.

In der Presse ist mehrfach berichtet worden, daß Verfassungsschutzbehörden Verdachtsindizien an Wirtschaftsunternehmen mitgeteilt hätten (ohne daß das vorgeschriebene Verfahren der Sicherheitsprüfung eingehalten worden sei). In den meisten Fällen richtete sich dieser Vorwurf gegen Landesämter für Verfassungsschutz; soweit das Bundesamt angesprochen war, habe ich keine Anhaltspunkte dafür festgestellt, daß Übermittlungen unter Verstoß gegen die dargestellten Prinzipien vorgekommen seien. Bei der Übermittlung von Erkenntnissen durch das BfV ist nicht zu verkennen, daß selbst ein mit Vorbehalten versehener Bericht einer Verfassungsschutzbehörde im Ergebnis den Betroffenen nachhaltig belasten kann. Die empfangenden Stellen werden das vorgelegte Material vielfach nicht mehr objektiv prüfen, sondern bereits die Tatsache, daß überhaupt Erkenntnisse vorliegen, zum Nachteil des Betroffenen verwerten.

Von dieser Erkenntnis ausgehend hat das OVG Berlin in seiner Entscheidung vom 18. April 1978 (Neue Juristische Wochenschrift 1978 S. 1644 ff) festgestellt, daß die Ämter für Verfassungsschutz ihre gesammelten Erkenntnisse erst dann an Dritte weitergeben dürfen, wenn diese insgesamt geeignet seien, die Beurteilung als „verfassungsfeindliche Bestrebungen" zu begründen. An den Wahrheitsgehalt der Informationen seien strenge Anforderungen zu stellen. Es dürften nur solche Tatsachen übermittelt werden, „die den Schluß einer verfassungsfeindlichen, die demokratischen Freiheiten zielstrebig untergrabenden Hetze oder eines tätlichen Angriffs zuverlässig" trügen (a. a. O. S. 1646). In allen anderen Fällen wären demnach die Ämter für Verfassungsschutz zwar nicht gehindert, weiter Daten zu sammeln und intern auszuwerten; sie müßten sie aber den anfragenden Stellen solange vorenthalten, bis sich der bloß vage Verdacht verfassungsfeindlicher Bestrebungen zum echten Zweifel verdichtet habe.

Damit können die Behörden für Verfassungsschutz über ihre sammelnde und auswertende Funktion hinaus faktisch Entscheidungen zum Beispiel von Einstellungsbehörden vorwegnehmen. Dies ist aus mehreren Gründen bedenklich. Die Einstellungsbehörden müssen ihre Entscheidung auf der Basis nur unvollständig verfügbaren Materials treffen (vgl. auch Wand, abweichende Meinung in BVerfGE 39, 334, 386, 390); die Mitarbeiter der Verfassungsschutzämter hingegen kennen die Betroffenen nicht persönlich, und ihnen fehlen häufig andere relevante Unterlagen (eine Folge davon, daß die Anfragen der Einstellungsbehörden bei Verfassungsschutzämtern nur der Auswertung dort bereits vorhandenen, im Rahmen des § 3 Verfassungsschutzgesetz gesammelten Materials dienen dürfen; eine eigenständige Aufgabe der Mitwirkung bei Einstellungen ist für das Bundesamt gesetzlich nicht festgelegt).

Dennoch halte ich im Ergebnis die Auffassung des OVG Berlin für zutreffend. Solange bei den Behörden für Verfassungsschutz lediglich geringe und nicht durch gewichtige Tatsache nachweisbare vage Verdachtsmomente an der Verfassungstreue eines Betroffenen bestehen, ist es meines Erachtens gerechtfertigt, sie anderen Stellen als Verfassungsschutzbehörden vorzuenthalten. Dies entspricht der freiheitlichen Konzeption des Grundgesetzes und dem Grundsatz der Verhältnismäßigkeit.

Nach einem Erlaß des Bundesministers des Innern an das BfV vom Juni 1978 dürfen im Rahmen von Einstellungsüberprüfungen ausschließlich solche Er-

kenntnisse mitgeteilt werden, die in einem eventuellen Verfahren gegen die Einstellungsbehörde auch gerichtsverwertbar sind. Der Ablehnungsbescheid kann vom Bewerber angefochten werden; innerhalb dieses Verfahrens besteht auch Rechtsschutz gegen unzulässige oder unrichtige Datenübermittlung durch das BfV an Einstellungsbehörden.

Außerdem dürfen nach diesem Erlaß Anfragen an das BfV nur erfolgen, wenn eine Einstellung des Bewerbers beabsichtigt ist. Das Bundeskabinett hat auch darauf hingewiesen, daß auf die bisher geübte routinemäßige Anfrage beim BfV verzichtet wird, wenn nach den Umständen des Einzelfalles offensichtlich kein Grund zu Zweifeln an der Verfassungstreue besteht (Beschluß vom 8. November 1978, Bulletin der Bundesregierung Nr. 131 vom 14. November 1978 Seite 1221). Diese Einschränkung der sogenannten „Regelanfrage" — die allerdings nicht gilt, wenn gleichzeitig eine Sicherheitsüberprüfung veranlaßt ist — entspricht dem Ziel des Datenschutzes, die Informationssammlung und -übermittlung auf das unbedingt notwendige Maß zu beschränken.

3.4.3.3 Zusammenarbeit der Polizeibehörden, insbesondere des Bundesgrenzschutzes, mit dem Bundesamt für Verfassungsschutz und anderen Nachrichtendiensten

Nach Artikel 35 GG haben sich alle Behörden des Bundes und der Länder gegenseitig Rechts- und Amtshilfe zu leisten. In § 3 Abs. 4 Verfassungsschutzgesetz ist diese Verpflichtung noch einmal für das Bundesamt für Verfassungsschutz wiederholt. Die Praxis der Unterstützung anderer Behörden durch das BfV ist im vorigen Abschnitt (3.4.3.2) behandelt worden. Die Art und Weise, in der die Amtshilfe anderer Stellen für das BfV praktiziert wird, war Gegenstand von Kritik. Aus dem BfV waren vor einiger Zeit Listen von Publikationen und Organisationen an die Grenzschutzdirektion Koblenz gegeben und von dort weitergeleitet worden, die nach Ansicht der beteiligten Beamten geeignet waren und dazu dienen sollten, den Polizeibeamten im Grenzschutzdienst Kenntnisse über extremistische Organisationen und für sie tätige Einzelpersonen zu vermitteln; Reisen solcher Personen sollten dem BfV gemeldet werden.

Diese Listen wurden vom Bundesminister des Innern zurückgezogen. Sowohl das Ministerium wie die Leitung des BfV haben erklärt, daß sie die Verbreitung dieser Listen als ungeeignet und schädlich ansehen. Nach Angaben der zuständigen Behörden wurden keine Erkenntnisse aufgrund dieser Listen an das BfV gemeldet oder dort gespeichert. Ich habe auch bei meinen Kontrollen keine Anhaltspunkte dafür gefunden, daß solche Meldungen erfolgt seien. Die Landesregierungen haben, soweit in den Landtagen entsprechende Anfragen gestellt wurden, die gleiche Auskunft erteilt.

Die rechtliche Problematik der Zusammenarbeit von Polizeibehörden und BfV folgt aus dem Spannungsverhältnis zwischen Amtshilfepflicht und der Versagung polizeilicher Befugnisse für das BfV (§ 3 Abs. 3 Satz 1 Verfassungsschutzgesetz). Sie ist gegenwärtig Gegenstand von Erörterungen einer Arbeitsgruppe im Bundesministerium des Innern; ein Ergebnis ist für die nächste Zeit angekündigt. Ich werde mich mit den Feststellungen dieser Arbeitsgruppe auseinandersetzen und in dieser Sache weitere Gespräche mit dem BfV führen. Nur dann, wenn Erkenntnisse, die von Polizeidienststellen aufgrund polizeilicher Befugnisse gewonnen wurden, dem BfV und den anderen Nachrichtendiensten überhaupt übermittelt werden dürfen, ist die Möglichkeit einer rechtmäßigen Datenverarbeitung dieser Erkenntnisse gegeben; darüber hinaus müssen die weiteren Voraussetzungen, insbesondere die Erforderlichkeit der Datenverarbeitung vorliegen.

3.4.3.4 Gegenstand meiner Prüfung und bisherige Prüfungsergebnisse

Das BDSG schützt in Dateien gespeicherte und aus Dateien übermittelte personenbezogene Daten. Akten und Aktensammlungen gehören nach § 2 Abs. 3 Nr. 3 BDSG nicht zu den Dateien im Sinne des Gesetzes, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Dadurch ist auch meine Kontrollbefugnis begrenzt, soweit nicht die Einhaltung „anderer Vorschriften über den Datenschutz" (§ 19 Abs. 1 Satz 1 BDSG) zu kontrollieren ist.

Beim BfV erfüllt insbesondere das nachrichtendienstliche Informationssystem NADIS den Dateibegriff. An NADIS sind das BfV, dem eine Leitfunktion zukommt, die Landesbehörden für Verfassungsschutz, die Staatsschutz-Abteilung des BKA sowie der BND und der MAD (die letztgenannten jedoch nicht im on-line-Verkehr) angeschlossen. Bisher wird NADIS in der Form einer Hinweisdatei geführt. Es enthält neben dem Namen und weiteren Angaben zur Identifizierung einer Person (zum Beispiel Geburtstag, Geburtsort, Staatsangehörigkeit, Anschriften, Telefonnummern, Kraftfahrzeugkennzeichen, Konto- und Schließfachnummern) die Aktenzeichen von Unterlagen, die bei einem oder mehreren NADIS-Partnern über die Person oder die Organisation geführt werden. Über den Inhalt der Akten enthält das System keine Aussage. Allerdings hat das Aktenzeichen für den Fachkundigen eine gewisse Aussagekraft.

Wenn ich kontrollieren will, ob die Speicherung der Daten in NADIS nach § 9 Abs. 1 BDSG zulässig ist, muß ich den Inhalt der zugrundeliegenden Akten kennen. Das Recht, diese Akten und sonstige Unterlagen einzusehen, gibt mir § 19 Abs. 3 Satz 2 BDSG. Die Speicherung personenbezogener Angaben im NADIS begegnet keinen Bedenken, wenn die Informationssammlung durch die gesetzliche Aufgaben- und Befugniszuweisung gedeckt ist (vgl. oben 3.4.3.1). Da NADIS als Hinweisdatei angelegt ist, muß die Speicherung selbst dann als gerechtfertigt angesehen werden, wenn gegen einen Teil des Akteninhalts Bedenken bestehen. Die Bedenken werden mit den zuständigen Vertretern des BfV besprochen.

Der Bundesbeauftragte kann jedoch nur die Akten überprüfen, die von Bundesbehörden geführt werden. Stellt er fest, daß NADIS einen Hinweis auf Akten einer Landesbehörde enthält, muß insoweit

die Kontrolle durch den Beauftragten oder den Ausschuß für Datenschutz des Landes erfolgen. Auch für den Fall, daß über eine Person Akten sowohl bei einer Bundes- als auch bei einer Landesbehörde oder bei mehreren Landesbehörden geführt werden, muß noch — im Einvernehmen mit den beteiligten Aufsichtsbehörden der Länder — ein Verfahren gegenseitiger Hilfe entwickelt werden, das die Kontrolle ermöglicht, ohne Sicherheitsbelange zu beeinträchtigen.

Von den Einzelzuschriften, die sich mit dem Datenschutz im Bereich der öffentlichen Verwaltung befaßten, bezog sich die Mehrzahl auf den Verfassungsschutz und die Tätigkeit der Polizei. Von einzelnen Ausnahmen abgesehen, enthielten die Eingaben keine Beschwerden über konkrete Mißbrauchsfälle. Die Mehrzahl der Einsender hat festzustellen, was bei den Behörden für Verfassungsschutz über sie gespeichert ist (vgl. dazu unter 3.4.7.3). Andere berichteten über einzelne Geschehnisse oder eigene Verhaltensweisen (zum Beispiel Teilnahme an Demonstrationen) und äußerten die Befürchtung, dies könnte gespeichert worden sein und ihnen später zum Nachteil gereichen.

Ich habe in allen Fällen von den mir gesetzlich übertragenen Kontrollbefugnissen Gebrauch gemacht und die Akten durch einen damit besonders beauftragten Mitarbeiter einsehen lassen. Eine zum jeweiligen Überprüfungszeitpunkt rechtsfehlerhafte Speicherung konnte ich nicht feststellen. Zur Bewertung dieses Ergebnisses ist jedoch anzumerken, daß die Zahl der auf diese Weise durchgeführten Kontrollen noch gering ist und daß eine umfassende Nachprüfung in vielen Fällen schon deshalb nicht möglich war (und ist), weil der für eine intensive Sachverhaltserforschung nötige Dialog mit dem Betroffenen wegen des Auskunftsverweigerungsrechts der Sicherheitsbehörden nicht stattfinden darf (vgl. auch 3.4.7.3). Soweit in Eingaben konkrete Anhaltspunkte für die Bewertung des Sachverhalts angegeben waren, wurde ihnen nachgegangen (dies war vor allem dann möglich, wenn die Betroffenen wußten, daß eine polizeiliche oder Verfassungsschutz-Maßnahme stattgefunden hat, insbesondere bei Sicherheitsüberprüfungen). In der Regel waren jedoch keine konkreten Umstände angegeben, sondern nur allgemeine Befürchtungen, die sich auf Presseveröffentlichungen über rechtswidrige Kontrollmaßnahmen (wie die erwähnten „Grenzschutzlisten") stützten.

In einigen Fällen ist eine weitere Speicherung und Aufbewahrung der damit verbundenen Akten meines Erachtens nur noch für einen relativ kurzen Zeitraum vertretbar. Ich werde diese Fälle nach Ablauf einer bestimmten Frist wieder aufgreifen und sodann prüfen, ob dem BfV weitere Erkenntnisse vorliegen, die die Annahme einer verfassungsfeindlichen Aktivität zu rechtfertigen vermögen. Sollte dies nicht der Fall sein, werde ich auf eine Löschung der Eintragung und Vernichtung der Akte hinwirken. Ähnliche Fälle liegen mir beim Bundeskriminalamt vor, auf das im folgenden einzugehen ist. Im übrigen steht diese Methode der Kontrolle im Zusammenhang mit der Fortentwicklung bereichsspezifischer Datenschutzvorschriften, auf die ich unter 3.4.7.2 zurückkomme.

Besonderer Erwähnung bedarf der im Berichtsjahr aufgekommene Verdacht, Behörden für Verfassungsschutz unternähmen in öffentlichen Bibliotheken eine generelle Kontrolle des Ausleihverkehrs (mit dem Ziel einer Feststellung von Personen, die „extremistische" Literatur entleihen). Ich bin allen Hinweisen nachgegangen, die sich auf eine solche eventuelle Tätigkeit des BfV bezogen, habe jedoch keine Bestätigung gefunden. Für den Landesbereich ist u. a. der Hessische Datenschutzbeauftragte zu dem gleichen Ergebnis gekommen (VII. Tätigkeitsbericht zu 5.2). Doch habe ich diesen Fall zum Anlaß eines Rundschreibens an die obersten Bundesbehörden genommen und dort darauf hingewiesen, daß ich eine Erforschung des Leseverhaltens von Bibliotheksbenutzern in der Tat für unzulässig hielte. Um eventuellen Mißbräuchen vorzubeugen, habe ich empfohlen, Angaben über den Ausleihvorgang nach Rückgabe der entliehenen Büchern nicht nur zu sperren, sondern sie gemäß § 14 Abs. 3 Satz 1 BDSG sogleich zu löschen, da sie dann nicht mehr erforderlich seien.

3.4.4 Bundeskriminalamt (BKA)

Im Bundeskriminalamt sind wie beim BfV die dort geführten Dateien Gegenstand meiner Kontrolle. Es handelt sich um die im kriminalpolizeilichen Informationssystem INPOL zusammengefaßten Datenbanken einschließlich des besonderen Systems PIOS (Personen, Institutionen, Organisationen, Sachen), das in erster Linie zur Bekämpfung des Terrorismus aufgebaut und inzwischen auf den Bereich der Rauschgiftkriminalität ausgedehnt worden ist (zur Zusammenarbeit mit anderen Stellen in diesem Bereich vgl. unten 3.4.4.2).

Die überprüften Einzelfälle haben bisher keinen Anlaß zur Beanstandung gegeben. Allerdings liegen mir zwei Fälle vor, bei denen nach Ablauf einer gewissen Zeit geprüft werden muß, ob die Speicherung noch erforderlich ist.

Erste Kontaktgespräche und bisher durchgeführte Prüfungen haben gezeigt, daß auch im BKA uneingeschränkte Bereitschaft zur Zusammenarbeit besteht. Meinungsverschiedenheiten werden allerdings wegen des auch hier gegebenen Zielkonflikts nicht ausbleiben.

In den folgenden Unterabschnitten soll auf Grundsatzprobleme der Informationsverarbeitung im Bereich des BKA hingewiesen werden, die einer differenzierteren Lösung bedürfen, als es jetzt offenbar der Praxis entspricht. Obwohl ich hierbei nur zu den polizeilichen Gegebenheiten beim Bund Stellung nehmen kann, ist zu bemerken, daß die Probleme sich für den Länderbereich im Prinzip zum Teil ähnlich stellen dürften.

3.4.4.1 Verwertungsverbot nach § 49 Bundeszentralregistergesetz (BZRG) und Auskunftspflicht des BKA

Das BKA unterrichtet (ähnlich wie die Landeskriminalämter) andere Polizeibehörden gemäß § 2 BKA-Gesetz grundsätzlich über Straftaten auch dann, wenn die betreffende Verurteilung bereits ge-

tilgt ist. § 49 BZRG bestimmt hingegen, daß eine Straftat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden dürfen, wenn die Eintragung über eine Verurteilung im Register getilgt oder zu tilgen ist.

Ausnahmen von diesem Verwertungsverbot läßt das BZRG nur in engen Grenzen zu (§ 49 Abs. 2 und § 50). Es soll nicht verkannt werden, daß auch Kenntnisse über inzwischen getilgte Verurteilungen für die Tätigkeit der Polizeibehörden — und zwar sowohl die Gefahrenabwehr wie die Strafverfolgung — von Bedeutung sein können. Doch wird man das Verhältnis der Mitteilungspflicht nach dem BKA-Gesetz zum Verwertungsverbot nach dem BZRG im Lichte des Datenschutzes restriktiver sehen müssen, als es gegenwärtig offenbar geschieht. Auch wenn das BDSG bisher formell nur die Informationsverarbeitung in oder aus Dateien betrifft, geht das Gebot des Datenschutzes materiell, wegen seiner verfassungsrechtlichen Basis in Artikel 1 und 2 GG, über diesen Bereich hinaus. Daß auch der Gesetzgeber des BZRG das Konkurrenzverhältnis zwischen polizeilichen Bedürfnissen und dem durch die Tilgungsvorschriften geförderten Rehabilitationsinteresse gesehen hat, ergibt sich aus den Ausnahmeregeln in § 50, wo (in Absatz 1 Nr. 1) eine Abwägung zu Gunsten zwingender Interessen der Sicherheit der Bundesrepublik und ihrer Länder vorgenommen worden ist und (in Absatz 1 Nr. 4) eine ebensolche Abwägung bei der Zulassung zu einem Beruf oder Gewerbe, der Einstellung in den öffentlichen Dienst oder der Erteilung waffenrechtlicher Erlaubnisse vorgeschrieben wird. Auch § 50 Abs. 2 (Zulassung der Berücksichtigung von Verkehrsstraftaten bei der Erteilung oder Entziehung von Fahrerlaubnissen) zeigt, daß der Gesetzgeber hochrangigen Interessen der Allgemeinheit entgegenkommen wollte, stützt aber andererseits die Schlußfolgerung, daß darüber hinaus keine Durchbrechungen des Verwertungsverbotes zulässig sein sollten. Aus Anlaß eines konkreten Falles habe ich das Bundesjustizministerium und das Bundesinnenministerium um Stellungnahme zu dieser Grundsatzproblematik ersucht. Das Ergebnis dieser Anfrage wird auch in die Arbeiten an den neuen Richtlinien für die kriminalpolizeiliche Sammlung personenbezogener Daten einfließen müssen (vgl. 3.4.7.2).

Darüber hinaus bedarf die Praxis der polizeilichen Sammlung von Informationen über Verfahren, die nicht zur Verurteilung geführt haben und deshalb nicht den Regeln des BZRG unterliegen, der Überprüfung.

3.4.4.2 Probleme des Verbundes verschiedener Informationssysteme

Es bedarf der Klärung, ob die bestehenden Zugangsrechte des Bundesamtes für Verfassungsschutz zu Informationssystemen des Bundeskriminalamtes für die rechtmäßige Aufgabenerfüllung wirklich erforderlich sind. Zwar erkennen die Sicherheitsbehörden das Prinzip an, daß sie nur die Informationen beanspruchen können, die für ihre jeweiligen Aufgaben benötigt werden, aber die Anwendung dieses Prinzips ist teilweise streitig. Ich habe die Frage aufgeworfen, weshalb die Terrorismusabteilung des BfV ohne weiteres (d. h.: ohne Möglichkeit des BKA, die Erforderlichkeit im Einzelfall zu prüfen) auf das Informationssystem PIOS (Bereich Terrorismus) des BKA zurückgreifen kann. Die *generelle* Berechtigung hierzu wäre trotz der Tatsache, daß das BfV auch Aufgaben auf dem Feld der Terrorismusbekämpfung zu erfüllen hat, nur dann gegeben, wenn diese Aufgabenstellung sich vollkommen deckte. Da dies nicht der Fall ist, dürfen Informationen vom BKA nur im Einzelfall nach einer zumindest pauschalen Erforderlichkeitsprüfung an das BfV übermittelt werden. Umgekehrt bestehen erhebliche Bedenken gegen den Anschluß des BKA an NADIS. Das BKA hat keine nachrichtendienstliche Aufgaben.

Die Bedenken gelten erst recht für den über das Nachrichtensystem PIOS hinausgehenden Zugang des BfV zum Datenbestand „Polizeiliche Beobachtung". Dem BfV sind polizeiliche Befugnisse versagt. Es erscheint daher fragwürdig, ob angesichts dieser Trennung von Polizei und Verfassungsschutz die aufgrund polizeilicher Befugnisse gewonnenen Erkenntnisse den Ämtern für Verfassungsschutz überhaupt zugänglich sein dürfen.

Das BfV beruft sich auf die gesetzliche Verpflichtung der anderen Behörden zur Amtshilfe. Wie weit diese Pflicht geht, ist zur Zeit Gegenstand von Überlegungen der im Bundesministerium des Innern gebildeten Arbeitsgruppe (vgl. 3.4.3.3).

3.4.4.3 Kriterien für die Aufnahme in das System PIOS

So bald wie möglich sollten allgemeine Kriterien dafür erarbeitet werden, wann eine Einspeicherung in das Nachrichtensystem PIOS gerechtfertigt ist und unter welchen Voraussetzungen dort Daten zu löschen sind. Bisher ist nur festgelegt, auf welchen Kriminalitätsbereichen das System PIOS eingesetzt wird; dies kann heute nicht mehr genügen. Entsprechende Vorarbeiten sind — unter Beteiligung meiner Dienststelle — im Gange.

Es muß allerdings erwähnt werden, daß sich das System PIOS durch eine strenge Zugriffskontrolle auszeichnet. Die Zugriffsberechtigung erhalten nur bestimmte Personen bei den angeschlossenen Dienststellen; ihnen allein werden die Berechtigungscodes zugeteilt (Übermittlung als Verschlußsachen). Die Berechtigung betrifft jeweils nur ein Abrufgerät. Sind bei einer zugangsberechtigten Dienststelle mehrere Personen zugriffsberechtigt, so ist der Sicherheitscode des einzelnen Berechtigten den anderen nicht bekannt. Vom übrigen kriminalpolizeilichen Informationssystem (INPOL) ist das System PIOS abgeschottet. Dies gilt auch für die Aktenführung.

3.4.4.4 Polizeiliche Beobachtung („beobachtende Fahndung")

Das Speichern personenbezogener Daten ist nach § 9 Abs. 1 BDSG nur zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist. Daher prüfe ich auch, ob die handelnden Stellen

ihren gesetzlich bestimmten Aufgabenkreis einhalten. Für die polizeiliche Personenbeobachtung („beobachtende Fahndung" [„Befa"]) bestehen insofern erhebliche Zweifel. Das Bundeskriminalamt ist nach § 5 BKA-Gesetz auf die Strafverfolgung beschränkt (mit Ausnahme des hier nicht interessierenden Personen- und Objektschutzes nach § 9 BKAG). Die polizeiliche Beobachtung läßt sich aber vielfach nur als Maßnahme der Gefahrenabwehr bzw. vorbeugenden Verbrechenbekämpfung rechtfertigen. Mag auch die Notwendigkeit solcher „beobachtender Fahndung" in vielen Fällen aus polizeitaktischen Überlegungen heraus gegeben und unter Umständen eine Rechtsgrundlage für das Tätigwerden von Polizeibehörden vorhanden sein, so fehlt es hieran jedenfalls, wenn das Bundeskriminalamt auf diese Weise tätig werden will. Auch unter dem Aspekt der Strafverfolgung ist die rechtliche Zulässigkeit entsprechender Maßnahmen nicht hinreichend gesichert. Bestehende innerdienstliche Vorschriften können eine heimliche Beobachtung von Bürgern nicht im Außenverhältnis, dem Betroffenen gegenüber, rechtfertigen. Da die Speicherung personenbezogener Daten nur zulässig ist, wenn ihre Erhebung rechtmäßig erfolgt, ist dies auch datenschutzrechtlich relevant. Wenn trotz dieser Bedenken an der beobachtenden Fahndung festgehalten werden soll, ist der Gesetzgeber aufgerufen, den rechtlichen Rahmen dafür genau abzustecken.

3.4.5 Geschäftsbereich des Bundesministers der Verteidigung einschließlich des militärischen Abschirmdienstes

Im Bereich des Bundesministers der Verteidigung hat es bisher keinen Anlaß zu Beanstandungen bei der Überprüfung von Einzelfällen der Datenverarbeitung gegeben.

In einer Eingabe ist eine Verletzung der Datensicherheit im Bereich des Wehrersatzwesens behauptet worden; die Ermittlungen hierzu sind noch im Gange.

Allerdings muß im Geschäftsbereich des Verteidigungsministers auf Verbesserungen hinsichtlich der Löschungspraxis hingewirkt werden. Dies gilt gleichermaßen für die Tätigkeit des MAD wie die der Wehrersatzbehörden. Bei letzteren ist insbesondere eine Revision der bisherigen Praxis der Speicherung von Daten Wehrpflichtiger erforderlich, die gemäß § 24 Abs. 3 Wehrpflichtgesetz nicht der Wehrüberwachung unterliegen (das sind die vom Wehrdienst dauernd ausgeschlossenen, vom Wehrdienst befreiten und die als Kriegsdienstverweigerer anerkannten Wehrpflichtigen). Entsprechende Anregungen habe ich auf Grund konkreter Einzelfälle bereits gemacht. Im Bundesministerium der Verteidigung wird die Notwendigkeit entsprechender Maßnahmen anerkannt.

3.4.6 Bundesnachrichtendienst

Für den Bereich des BND hat es noch keine Einzelbeschwerden gegeben. Dies dürfte damit zusammenhängen, daß dieser Dienst primär Sachdaten und nicht personenbezogene Daten sammelt und sein Aktionsfeld vorwiegend außerhalb der Bundesrepublik Deutschland liegt.

Ich habe mich über die Tätigkeit des BND allgemein informiert und Fragen, die unter Aspekten des Datenschutzes von Belang sind, mit Vertretern des Dienstes und dem Bundeskanzleramt besprochen. Aus Anlaß von Pressemeldungen über Methoden der Postkontrolle durch den BND habe ich weitere Informationen eingeholt. Dabei ergab sich Übereinstimmung darüber, daß die Weitergabe personenbezogener Daten, die aus Maßnahmen der Postkontrolle gewonnen werden, nur in den engen Grenzen von § 3 Abs. 2 bzw. § 7 Abs. 3 des Gesetzes zu Artikel 10 GG zulässig ist, darüber hinaus also keine Amtshilfe des BND für andere Behörden geleistet werden darf.

Wie beim MAD muß auch hier auf das unter rechtsstaatlichen Aspekten bedenkliche Fehlen einer klaren rechtlichen Absicherung der Tätigkeit des Dienstes hingewiesen werden. Zwar sind die Nachrichtendienste mittlerweile in mehreren Gesetzen erwähnt, und ihre Tätigkeit ist auch im BDSG als rechtmäßig vorausgesetzt, doch ersetzt dies die erforderliche gesetzliche Aufgaben- und Befugniszuweisung ebensowenig wie es die innerdienstlichen Verwaltungsvorschriften tun. Lediglich in dem Bereich, der vom Gesetz zu Artikel 10 GG erfaßt wird, bestehen — zumindest abstrakt — klare rechtliche Verhältnisse. Die übrigen als Eingriff in die Rechtssphäre zu qualifizierenden Maßnahmen der Nachrichtendienste bedürfen grundsätzlich einer *gesetzlichen* Ermächtigungsgrundlage; nur unter dieser Voraussetzung dient auch das Speichern der gesammelten Daten der rechtmäßigen Aufgabenerfüllung im Sinne von § 9 Abs. 1 BDSG. Jedenfalls wird meine — vom Gesetzgeber auch für diesen Bereich vorgesehene — Prüfungstätigkeit durch diese Situation erheblich erschwert.

3.4.7 Gleichartige Probleme der Sicherheitsbehörden und künftig anzustrebende Verbesserungen

3.4.7.1 Verfahren zur Löschung von Daten

Ich habe bereits unter 3.4.3.1 auf die datenschutzrechtlichen Probleme hingewiesen, die sich daraus ergeben, daß zum Beispiel das BfV entsprechend seinem Auftrag auch Daten über Personen speichern muß, bei denen sich nach kurzer oder längerer Zeit erweist, daß sie keine „Bestrebungen" im Sinne des Verfassungsschutzgesetzes verfolgen. Ähnliche Probleme ergeben sich im Bereich der Polizei bei Personen, gegen die ermittelt wird und deren Unschuld sich später herausstellt. Allein die Tatsache, daß gegen diese Personen ermittelt worden ist, kann in mancherlei Beziehung zu einer Belastung für sie werden. Die Speicherung derartiger Angaben in automatisierten Informationssystemen führt — wegen der damit notwendigerweise verbundenen Verkürzung der Informationen — zu zusätzlichen Belastungen. Hinzu kommt, daß die Informationen nunmehr weithin, teilweise sogar bundesweit verfügbar sind.

Für die speichernden Behörden erwächst hieraus allgemein die Verpflichtung, ihre Bestände in angemessenen Zeitabständen darauf zu überprüfen, ob und welche Daten zu vernichten sind. Wie jede aktenführende Verwaltung hat sich auch die eine oder andere Sicherheitsbehörde bereits in der Vergangenheit um der eigenen Entlastung willen von manchen alten Beständen befreit; eine vollständige Bestandsüberprüfung in nicht zu langen Abständen ist aber, soweit ich sehe, in keinem Bereich bisher realisiert. Zur Erledigung dieser Aufgabe bedarf es eines einvernehmlichen Vorgehens aller beteiligten Stellen nicht nur beim Bund, sondern auch in den Ländern.

Erste Initiativen in dieser Richtung sind bei allen Sicherheitsbehörden des Bundes, zum Teil auf meine Anregung, eingeleitet worden. Als Beispiel ist das System der Zeitspeicherung zu nennen, das beim Bundesamt für Verfassungsschutz beabsichtigt ist (dazu unten 3.4.7.2), ebenso die dort begonnene Erarbeitung von Kriterien für die Überprüfung und Löschung personenbezogener Daten von Amts wegen. Ähnliche Bemühungen bestehen bei den anderen meiner Kontrolle unterliegenden Bundesbehörden. Beim Bundeskriminalamt werden gegenwärtig neue Richtlinien über die Führung von Kriminalakten vorbereitet; darin ist die automatische Löschung von Dateihinweisen in Verbindung mit der Vernichtung der entsprechenden Akten nach abgestuften Fristen unter bestimmten Voraussetzungen vorgesehen.

Unklarheit ist in letzter Zeit darüber entstanden, ob das Verfahren der Löschung unrichtiger oder sonst zu löschender Daten bei den Sicherheitsbehörden richtig durchgeführt wird. Dabei ist davon auszugehen, daß § 2 Abs. 2 Nr. 4 BDSG unter „Löschen (Löschung)" „das Unkenntlichmachen gespeicherter Daten" versteht, und zwar „ungeachtet der dabei angewendeten Verfahren". Unter Löschen muß also verstanden werden, daß der Datenträger nicht nur zur Wiederverwendung freigegeben wird, sondern daß vorher die Aufzeichnungen selbst vernichtet werden, das heißt, daß auch deren magnetische Markierungen, die elektrische Impulse auslösen, restlos getilgt werden. Für Magnetbänder und -platten ist also eine Beseitigung der Aufzeichnungen auf den entsprechenden Datenspuren vorzunehmen.

Wenn also zum Beispiel ein Anspruch auf Löschung erkennungsdienstlicher Unterlagen gegenüber dem BKA besteht, müssen diese Aufzeichnungen restlos vernichtet werden. Ein entsprechender Anspruch des Betroffenen folgt aus § 14 Abs. 3 Satz 2 BDSG, der auch in anderen Fällen eine Löschung von Daten vorschreibt.

Die Verpflichtung zur so verstandenen vollständigen Löschung wird auch von den Sicherheitsbehörden grundsätzlich anerkannt. Aus Gründen der Datensicherung erfolgt die vollständige Löschung allerdings in Stufen. Zunächst wird das betreffende Datum in den auf Magnetplatten vorhandenen Datenbeständen des Echtzeitsystems durch den eingabeberechtigten Bediener gelöscht; dieser Löschungsvorgang wird sofort wirksam. Jedes Datenbanksystem braucht jedoch ein Sicherungsverfahren, um Daten, die durch technische oder andere Fehler verlorengegangen sind, rekonstruieren zu können. Dieses beruht bei allen Sicherungsbehörden auf dem gleichen Grundprinzip: In gewissen zeitlichen Abständen wird eine Kopie des Bestandes erstellt, und die Veränderungen des Datenbestandes werden von diesem Zeitpunkt an protokolliert. Bei Bedarf kann hieraus ein mit dem Originalbestand identischer Ersatzbestand erstellt werden, in dem dann auch die im Echtzeitsystem inzwischen angeordneten Löschungen vollzogen sind. Die Datenbestände des Sicherungsverfahrens werden für einige Wochen archiviert. Ein Zugriff auf diese Bestände ist nur in der Weise möglich, daß das Sicherungsband (bzw. die Sicherungsbänder) vollständig abgesucht wird, ein gezielter Zugriff auf Einzelinformationen ist also erheblich erschwert. Nach Ablauf der Frist werden auch diese Datenbestände unkenntlich gemacht.

Mit dem BKA wurde die Frage der Löschung erörtert. Daraufhin wurde dort die Frist zur Löschung der Sicherungsbänder auf vier Wochen verkürzt. Beim BND gilt das gleiche Verfahren der Löschung wie beim BKA. Bei BfV und MAD ergeben sich Besonderheiten insofern, als die Löschung dort zunächst nur im Auskunftsbestand erfolgt, nicht aber in den Protokollbändern, also den Aufzeichnungen über die erfolgten Eingaben und Abfragen. Nach Auffassung des BfV ist deren weitere Aufbewahrung für interne Sicherheitsmaßnahmen notwendig, zum Beispiel um unzulässige Löschungen und/oder Veränderungen im Auskunftsbestand rekonstruieren zu können. Für diese Bänder besteht ebensowenig wie beim BKA die Möglichkeit des gezielten Zugriffs auf Einzelinformationen. Für die an NADIS angeschlossenen anderen Behörden ist jeglicher Zugriff auf die Protokollbänder unmöglich, und innerhalb des BfV ist der Zugang streng eingegrenzt. Die Fachabteilungen des BfV können nicht selbst auf diese Protokollbänder und die dort noch vorhandenen Daten zugreifen, sondern den Zugang hat nur ein besonderes Referat, das unter engen Voraussetzungen im Ausnahmefall auf schriftlichen Antrag hin nach Genehmigung des Präsidenten des Amtes Auskünfte erteilt, die etwa notwendig sein könnten, um festzustellen, welche Stelle unzulässige Löschungen im Auskunftsbestand vorgenommen hat.

Man kann hier also von einer Art qualifizierter Sperrung sprechen. In eingehenden Erörterungen mit dem BfV ist klargestellt worden, daß diese besonders gesicherte Sperrung nicht ausreicht, wenn die Speicherung unzulässig war (§ 14 Abs. 3 Satz 2, erste Alternative BDSG).

Ungeachtet der technischen Schwierigkeiten müssen die entsprechenden Daten in diesem Fall auch auf dem Protokollband gelöscht werden. Die Unzulässigkeit kann sich nicht nur aus einem rechtskräftigen Urteil ergeben, sondern auch im Anschluß an eine Prüfung durch mich festgestellt werden. Im übrigen aber muß streng geprüft werden, ob die Erforderlichkeit der Aufbewahrung von Daten in den Protokollbändern nach Wegfall der Speicherung im Auskunftsbestand für *alle* Arbeitsbereiche des BfV noch fortbesteht. Sowie die Erforderlichkeit nicht mehr bejaht werden kann, muß auch insoweit die Lö-

schung erfolgen. Hierüber wird mit dem BfV weiter verhandelt.

Für den MAD ist die Situation, wie schon angedeutet, ähnlich wie für das BfV. Auch hier bin ich um weitere Verbesserungen in dem geschilderten Sinne bemüht. Entsprechende Erörterungen sind im Gange. Für Erkenntnisse, die auf Grund des Gesetzes zu Artikel 10 GG gewonnen werden, folgt die Pflicht zur vollständigen Löschung aus der bereichsspezifischen datenschutzrechtlichen Bestimmung des § 7 Abs. 4 G 10, wonach die Unterlagen zu vernichten sind, wenn sie nicht mehr zu den vom Gesetz vorgesehenen Zwecken benötigt werden. Über die Vernichtung ist eine Niederschrift zu fertigen.

3.4.7.2 Fortentwicklung des bereichsspezifischen Datenschutzes (Voraussetzungen der Löschung)

Die Klarstellung, daß vollständig gelöscht wird, wenn die weitere Aufbewahrung nicht mehr erforderlich ist, nützt wenig, wenn die speichernde Behörde die Erforderlichkeit mehr oder weniger unbegrenzt bejaht.

Deshalb ist es ein wichtiges Anliegen des bereichsspezifischen Datenschutzes für die Behörden der öffentlichen Sicherheit, geeignete Kriterien herauszuarbeiten und entsprechende Richtlinien und/oder gesetzliche Vorschriften zu formulieren, die eine Befristung der Speicherung bewirken. Hierbei ist sowohl an eine automatische Löschung von Amts wegen nach Fristablauf wie an die Einrichtung eines Verfahrens zu denken, das garantiert, daß die Daten regelmäßig auf ihre weitere Erforderlichkeit hin überprüft werden. Selbstverständlich könnten solche Verfahrensweisen die Einzelfallprüfung auf Antrag des Betroffenen — gegebenenfalls unter meiner Mitwirkung — vor Ablauf genereller Fristen nicht erübrigen; sie würden aber den Rechtsschutz des Bürgers erheblich verbessern und sich insofern als ein Stück „positiven Verfassungsschutzes" darstellen.

Ich verkenne nicht die Schwierigkeiten bei der Festlegung allgemeiner Kriterien für die Löschung. Es kann sich — namentlich im Bereich der Spionageabwehr — als notwendig erweisen, Informationen über Jahrzehnte hinweg aufzubewahren. Andererseits können zum Beispiel Daten über „Jugendsünden" schon nach relativ kurzer Zeit gelöscht werden. Erste wichtige Ansätze in Richtung einer solchen differenzierten Betrachtung sind erkennbar; sie sind auch unter dem Eindruck — um nicht zu sagen Druck — des BDSG entstanden. Das BfV plant die Einführung eines Systems der Zeitspeicherung. Die Realisierung hängt noch von technischen und finanziellen Bedingungen ab, die aber auf absehbare Zeit lösbar sein dürften. Bei diesem System wird nach Ablauf einer bestimmten, kurz bemessenen Zeit eine Erforderlichkeitsprüfung für die weitere Aufbewahrung durchgeführt bzw. veranlaßt.

Zusätzlich muß sichergestellt sein, daß auch die dazugehörigen Akten vernichtet werden, wenn die Daten in den Dateien gelöscht werden.

Die Entwicklung von Kriterien für automatische Löschung oder Überprüfung ist bei den Nachrichtendiensten schwieriger als beim BKA. Für dessen Bereich gelten gegenwärtig noch sogenannte „Bereinigungsrichtlinien" aus den Jahren 1969 und 1970, die den inzwischen deutlicher gewordenen rechtsstaatlichen Anforderungen nicht genügen, während zum Beispiel in Bayern nach strengeren Richtlinien über kriminalpolizeiliche Sammlungen (aus dem Jahre 1977) verfahren wird. Zur Zeit werden neue Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen entworfen, die zum Teil auf dem bayerischen Erlaß aufbauen. Es ist zu hoffen, daß diese Richtlinien bald verabschiedet werden.

Neben verwaltungsinternen bereichsspezifischen Datenschutzregelungen müssen auch zusätzliche gesetzliche Regelungen angestrebt werden, wie sie zum Beispiel in § 163 c Abs. 4 Strafprozeßordnung (Vernichtung von erkennungsdienstlichen Unterlagen unmittelbar nach Feststellung der Identität einer nicht verdächtigen Person) und in dem bereits mehrfach erwähnten § 7 Abs. 4 G 10 bestehen. Auch liegt ein Vorschlag der Innenministerkonferenz vom 25. November 1977 zu § 81 b StPO (erkennungsdienstliche Behandlung des Beschuldigten) vor, der Grundlage für ähnliche weiterführende Überlegungen sein könnte.

Auf weitere Sicht halte ich es für erforderlich, für polizeiliche und nachrichtendienstliche Informationssysteme eine in sich stimmige, den Freiheitsansprüchen der Bürger Rechnung tragende Gesamtkonzeption zu formulieren und in Gesetzesform zu bringen, statt Einzelkorrekturen an einer Vielzahl verstreuter Gesetzesbestimmungen vorzunehmen. Informationssysteme sind ein neuer Regelungsgegenstand, der bisher kaum als solcher erfaßt worden ist und auf den manche bestehenden Vorschriften nur schwer anwendbar sind (man denke an die Probleme im Bund-Länder-Verhältnis angesichts übergreifender On-line-Verbindungen mit gleichzeitiger Verfügbarkeit von Informationen an weit auseinanderliegenden Orten). Dabei müßten insbesondere auch Fragen des Anschlusses an solche Systeme, der Zugriffsberechtigung und des Datenaustausches berücksichtigt werden wie insbesondere auch die Rechte des Bürgers auf Auskunft über die eigenen Daten.

3.4.7.3 Praxis der Auskunftserteilung

Die in § 12 Abs. 2 Nr. 2 BDSG aufgeführten Sicherheitsbehörden sind nach § 13 Abs. 2 von der Verpflichtung zur Auskunftserteilung an den Betroffenen befreit. Mit dieser Regelung ist den Sicherheitsbedürfnissen der dort aufgezählten Behörden Rechnung getragen worden. Die Vorschrift ermächtigt sie zur Auskunftsverweigerung, verpflichtet aber nicht dazu. In der Praxis haben die Sicherheitsbehörden des Bundes diese Ermächtigung — soweit ersichtlich — genutzt, um nahezu ausnahmslos die Auskunft an den Betroffenen zu verweigern. Mehrere betroffene Bürger haben sich deshalb an mich gewandt. Nach dem Ergebnis meiner Überprüfungen habe ich erhebliche Zweifel, ob diese Praxis in allen Fällen geboten ist und ob sie im wohlverstandenen Interesse der Behörden selbst liegt.

Es gibt Fälle, in denen der Betroffene weiß, daß Daten über ihn gespeichert sind, etwa weil er einen Paß oder ein Kraftfahrzeug als gestohlen gemeldet hat oder weil er zum Umgang mit Verschlußsachen ermächtigt und aus diesem Grunde einer Sicherheitsüberprüfung unterzogen worden ist. Während des Verfahrens einer Sicherheitsüberprüfung kann es überdies vorkommen, daß dem Betroffenen weitere Informationen aus den Unterlagen des Verfassungsschutzes zugänglich gemacht werden müssen. Bestehen nämlich Bedenken gegen eine Ermächtigung, so sind ihm die Gründe insoweit zu eröffnen, als dies ohne Beeinträchtigung wichtiger Sicherheitsinteressen möglich ist. Schon gegenwärtig ist also eine völlige informatorische Abschottung dieser Stellen nicht möglich. Die Sicherheitsbehörden sollten prüfen, ob sie nicht auch in manchen Fällen, in denen der Betroffene nur vermutet, daß Daten über ihn gespeichert sind, eine Auskunft erteilen. Die Verweigerung der Auskunft läßt häufig den Verdacht entstehen, daß irgendwelche — negativ wirkenden — Informationen gespeichert seien, die der Betroffene nicht erfahren dürfe. Unsicherheit, Angst und Mißtrauen sind die Folge.

Die Behörden für Verfassungsschutz und andere Stellen mit hohem Geheimhaltungsinteresse rechtfertigen ihre generelle Auskunftsverweigerung damit, daß sie damit Ausforschungsversuche abwehren wollen. Dieses Anliegen ist grundsätzlich berechtigt, und eine Praxis etwa der Art, daß regelmäßig Auskunft erteilt würde, wenn nichts gespeichert ist, in allen übrigen Fällen aber die Auskunft verweigert würde, wäre mit diesem Ziel unvereinbar. Denn derjenige, der keine Auskunft erhielte, könnte dann schließen, daß irgendwelche Informationen über ihn gespeichert sind; schon dieses Wissen kann — namentlich im Bereich der Spionage — von erheblicher Bedeutung sein.

Trotzdem halte ich es für möglich, die Auskunftspraxis zu erweitern. So scheint es mir denkbar, Auskünfte über gespeicherte Informationen zu erteilen, wenn etwa Studenten befürchten, wegen politischer Aktivitäten nicht in den öffentlichen Dienst eingestellt zu werden. Ich bin mir darüber im klaren, daß eine erweiterte Auskunftspraxis das Risiko vermehrter gerichtlicher Auseinandersetzungen begründet; dies muß jedoch um der Rechtsstaatlichkeit willen hingenommen werden. Wenn es richtig ist, was sich nach meinen bisherigen — notwendigerweise unvollständigen — Einblicken in entsprechende Informationssysteme ergibt, daß nämlich keineswegs ein großer Teil der Bevölkerung von den Sicherheitsbehörden in irgendeiner Weise überwacht wird, dann würde eine weitergehende Offenlegung von Unterlagen der Sicherheitsbehörden vielen Menschen unbegründete Angst nehmen und die Arbeit dieser Behörden transparenter machen, was wiederum auch ihrer Aufgabenerfüllung zugute käme.

Daß solche Überlegungen nicht irreal sind, beweist das amerikanische Beispiel. Nach dem Freedom of Information Act (Public Law 93 — 502, 5 U. S. C. § 552, Übersetzung bei Joachim Scherer, Verwaltung und Öffentlichkeit, Baden-Baden 1978, Seite 96 ff.) hat jeder Anspruch ouf Offenlegung behördlicher Akten, wobei die Ausnahmen zwar zahlreich sind und auch eine Ausnahme im Interesse der nationalen Sicherheit gemacht ist, im Ergebnis aber nicht so weit zu gehen scheinen wie nach deutschem Recht. Nach Presseberichten haben die amerikanische Bundespolizei FBI und der Geheimdienst CIA eine erhebliche Zahl von Informationen offengelegt, zum Teil Vermerke über diffamierende Agentenmeldungen, die von den Betroffenen widerlegt worden sind.

Ich nehme in meiner Funktion als Sachwalter des Betroffenen seine Interessen so weit wie möglich wahr. Meine eigenen Ermittlungen auf Eingaben von Bürgern hin führen zwar zur Prüfung der Dateiinhalte und der dazugehörigen Akten, dabei sind mir jedoch, wie ich bereits oben zu 3.4.3.4 bemerkt habe, dadurch Grenzen gezogen, daß der Betroffene sich in der Regel zu den gespeicherten Informationen nicht äußern kann, die Prüfung also kein kontradiktorisches Verfahren, kein Dialog sein kann. Außerdem muß ich den Bescheid an den Betroffenen so abfassen, daß er nicht eine mittelbare Auskunft über den Inhalt der Datei ist, wenn die speichernde Stelle selbst diese Auskunft nicht erteilen will. In dem Bescheid auf eine Eingabe hin mache ich regelmäßig deutlich, daß die Mitteilung über das Ergebnis der Prüfung nicht als eine Antwort auf die Frage verstanden werden darf, ob Informationen bei bestimmten Behörden gespeichert seien. Mein Bescheid kann also bei der gegenwärtigen Rechtslage und Praxis der Sicherheitsbehörden den Betroffenen in den meisten Fällen keine Klarheit über die tatsächliche Seite der Verarbeitung ihrer Daten verschaffen, sondern nur eine rechtliche Beurteilung enthalten.

Einen Mittelweg stellt folgendes Verfahren dar, das ich bereits in einigen Fällen praktiziert habe: Wenn Bürger sich bei mir darüber beschwerten, sie seien aus Sicherheitsgründen oder mit ähnlichen Argumenten auf eine Bewerbung hin nicht angestellt worden oder hätten bestimmte Tätigkeiten nicht ausüben dürfen, und die Überprüfung ergab, daß nichts oder nichts Relevantes gegen den Betroffenen vorlag, habe ich im Einverständnis mit der speichernden Behörde, ggf. unter Einschaltung des zuständigen Landesdatenschutzbeauftragten, die Stelle, die den Betroffenen abgelehnt hatte, darauf hingewiesen, daß dies rechtswidrig oder mit falschen Gründen erfolgt sei, und um Abhilfe ersucht, ohne jedoch auch insoweit konkrete Hinweise zu geben. Ich bin mir zwar bewußt, daß ich mich hierbei am Rande meiner Kompetenzen bewege, doch halte ich diese „Hilfstätigkeit" im Interesse des Betroffenen für geboten und für gerechtfertigt, solange dadurch die Auskunftsverweigerungsrechte der Behörden nach § 13 Abs. 2 BDSG nicht umgangen werden.

Dasselbe gilt, wenn ich den Betroffenen neutral darauf hinweise, daß das für ihn negative Ergebnis einer Sicherheitsüberprüfung nicht für sich schon bedeutet, daß die Sicherheitsbehörden seine Person für ein aktives Sicherheitsrisiko hielten, sondern daß dies vielmehr — ohne jeglichen Vorwurf — auch darauf beruhen könnte, daß er Objekt sicherheitsgefährdender Tätigkeit anderer sei oder daß dies vermutet werden könne. Ich meine, daß gerade hierdurch den

Interessen der betroffenen Behörden und dem Datenschutz am meisten gedient ist. Ich werde deshalb versuchen, diesen Weg auszubauen, ohne dadurch ein Sicherheitsrisiko zu schaffen. Selbstverständlich ist dies nur in Zusammenarbeit mit den Sicherheitsbehörden möglich, da mit ihnen gemeinsam beurteilt werden muß, ob eine (Teil-)Auskunft überwiegende Sicherheitsinteressen verletzt oder nicht.

3.4.7.4 Vorlage von Verfassungsschutzakten in einem Rechtsstreit (Stellungnahme zu einer Verfassungsbeschwerde)

Das Bundesverfassungsgericht hat mir im Berichtszeitraum Gelegenheit gegeben, mich zu einigen Fragen im Zusammenhang mit einer anhängigen Verfassungsbeschwerde zu äußern. Gegenstand dieser Verfassungsbeschwerde ist die Weigerung eines Landesamtes für Verfassungsschutz, die über einen Bürger geführten Akten in einem Verwaltungsrechtsstreit nach § 99 Verwaltungsgerichtsordnung vorzulegen. Ich habe mich sowohl zu den mir gestellten Einzelfragen als auch zum generellen Problem des Zugangs zu Informationen des Verfassungsschutz geäußert.

Gegenwärtig wird im allgemeinen so verfahren wie in dem zur Entscheidung heranstehenden Einzelfall: Die Vorlage wird mit der Begründung verweigert, interne Akten des Verfassungsschutzes könnten grundsätzlich nicht an andere Behörden als die Ämter für Verfassungsschutz oder ihre Aufsichtsinstanzen herausgegeben werden, da ihr Inhalt Rückschlüsse auf die Organisation und die Arbeitsweise der Verfassungsschutzbehörden zulassen. Sie müßten deshalb „ihrem Wesen nach" (Text des § 99 VwGO) geheimgehalten werden. Es entspricht dieser Auffassung, daß im Bundesdatenschutzgesetz den Behörden für Verfassungsschutz generell das Recht eingeräumt ist, den Betroffenen die Auskunft über die über sie gespeicherten Daten zu verweigern.

Es gibt aber, wie oben zu 3.7.4.3 ausgeführt, einige Fälle, in denen die Geheimhaltung nicht zwingend erscheint, so wenn der Betroffene weiß, daß über ihn Daten gespeichert sind. Wird auch in diesen Fällen die Auskunft generell verweigert, so kann diese Praxis dazu beitragen, das ohnehin weit verbreitete Mißtrauen in die Sicherheitsbehörden ohne Grund weiter zu verstärken.

Vielfach wird es auch möglich sein, die Akten in einen geheimhaltungsbedürftigen und in einen offenen Teil zu trennen (noch besser: die Akten von vornherein so anzulegen, daß eine Aufteilung ohne weiteres möglich ist). In den offenen Teil könnten Daten aus allgemein zugänglichen Quellen (z. B. Zeitungsausschnitte, Flugblätter oder andere Unterlagen, deren Existenz für den Betroffenen offenkundig ist, wie etwa Strafregisterauszug, Paßverlustmeldung) aufgenommen werden.

In der Stellungnahme zu der Verfassungsbeschwerde bin ich auch auf die verschiedenen Ansätze einer Kontrolle der Informationsverarbeitung in diesem Bereich eingegangen. Da die Kontrolle durch den Betroffenen gesetzlich weitgehend ausgeschlossen ist, die der Gerichte durch die Beschränkung der Vorlagepflicht nach § 99 VwGO praktisch begrenzt ist, haben andere Kontrollansätze besondere Bedeutung. Die Aufsicht über die Verfassungsschutzämter durch die vorgesetzte Behörde stellt zwar keine externe Kontrolle im strengen Sinne dar; es wäre aber unrealistisch anzunehmen, daß die handelnde Behöerde und die Fachaufsichtsinstanz regelmäßig dieselbe „Politik" verfolgen.

Die Ämter für Verfassungsschutz sind bereits durch Dienstanweisungen, Dienstvorschriften und Richtlinien sowie Einzelerlasse der Innenminister in vielfältiger Weise gebunden. Berichts- und Vorlagepflichten und regelmäßige Information der aufsichtführenden Stellen sollen es diesen ermöglichen, sich auch rechtzeitig in die Behandlung von Einzelfällen einzuschalten, wenn und soweit es um die Einhaltung rechtsstaatlicher Grenzen für die Tätigkeit des Verfassungsschutzes geht (vgl. oben 3.4.3.1). Tatsächlich werden solche Einwirkungsmöglichkeiten auch in erheblichem Umfange wahrgenommen. Es wird abzuwarten sein, wie sich darüber hinaus die Kontrolle durch die parlamentarische Kontrollkommission auf Grund des Gesetzes vom 11. April 1978 (BGBl. I S. 443) auswirkt. Über meine eigene Kontrolle habe ich oben (3.4.3.4) berichtet. Zu erwägen wäre darüber hinaus die Einschaltung eines unabhängigen „Datentreuhänders", der über die Offenlegung von Verfassungsschutzakten oder Teilen daraus zu entscheiden hätte. In Betracht käme eine Stelle oder eine Persönlichkeit, die unabhängig und am Verfahren unbeteiligt sein müßte. Die Einsetzung eines solchen neutralen Dritten hätte den Vorteil größerer Objektivität. Freilich erscheint es zweifelhaft, ob ein solcher Treuhänder bereit wäre, sich über ein Votum der beteiligten Behörde und unter Umständen der obersten Dienstbehörde hinwegzusetzen, wenn diese auf Grund ihrer überlegenen Sachkenntnis darlegen, daß die Akten aus Sicherheitsgründen geheimgehalten werden müßten.

Ich habe gegenüber dem Bundesverfassungsgericht ausgeführt, daß Verfahrensbeteiligte einschließlich der Richter als „Datentreuhänder" ausscheiden müßten, weil es mit den Grundsätzen der Gerichtsverfassung und des Prozeßrechts nicht vereinbar sei, wenn man das Gericht umfassender informieren wolle als die Parteien.

Auch Vertreter der Anwaltschaft haben sich in diesem Sinne geäußert. Inzwischen bin ich aber auf die amerikanische Praxis aufmerksam geworden, die Entscheidung über die Vorlage von Verwaltungsunterlagen durch das Gericht „in camera" treffen zu lassen. Nach dem Freedom of Information Act (s. o. 3.4.7.3) entscheidet das Gericht bei Beschwerden über die Verweigerung der Aktenvorlage und kann zu diesem Zweck den Inhalt der Behörden akten in nicht-öffentlicher Verhandlung prüfen, um festzustellen, ob diese Akten oder ein Teil davon auf Grund einer der in diesem Gesetz vorgesehenen Ausnahmen zurückgehalten werden muß (vgl. Joachim Scherer a. a. O. S. 81 ff.).

Ich werde auch diesen Problemkreis der Offenlegung von geheimen Unterlagen gegenüber den Betroffenen weiter beobachten.

3.5 Sozialverwaltung, Gesundheitswesen

3.5.1 Problemüberblick

Die soziale Sicherung umfaßt, um nur einige Beispiele zu nennen, die großen Bereiche der Sozialversicherung — die Rentenversicherung, die Krankenversicherung und die Unfallversicherung —, die Sicherung vor und bei Arbeitslosigkeit, die Sozialhilfe und die sonstigen Altersversorgungen und Alterssicherungen.

Das auch für Fachleute nur schwer überschaubare Netz sozialer Sicherung hat enge Verbindungen zu Teilen des Gesundheitswesens, zu Ärzten, Apothekern, zu deren Verbänden, zu Krankenhäusern und zur medizinischen Forschung. Zwischen den einzelnen Sozialversicherungsträgern, der Bundesanstalt für Arbeit, den Kassenärztlichen Vereinigungen und anderen Stellen findet ein intensiver Datenaustausch statt. Die umfassende Verwaltung sozialer und individueller Entfaltungschancen und die Tatsache, daß nahezu jeder Bürger von Handlungen und Informationsvorgängen auf diesen Gebieten betroffen ist, machen den Bereich der sozialen Sicherung zu einem der Schwerpunkte in der Arbeit des BfD.

Selbst der Fachöffentlichkeit ist die praktische Bedeutung des Datenschutzes hier lange verborgen geblieben. Erst allmählich wird allgemein bewußt, daß die Träger der sozialen Sicherung gleichsam über ein zweites Melderegister verfügen, das vielfach aktueller ist als das der Meldebehörden. Es enthält zum Teil höchst sensible Daten über fast alle Bürger und verfügt mit der Versicherungsnummer über einen Identifizierungsschlüssel, welcher eine Vielzahl von Verknüpfungen ermöglicht.

Die Datenstelle der Rentenversicherung (DSRV) in Würzburg, die vom Verband Deutscher Rentenversicherungsträger betrieben wird, speichert einige Grunddaten von ca. 45 Millionen Versicherten. Sie ist eine Clearingstelle mit umfassenden Aufgaben des Datenaustausches innerhalb der Rentenversicherung und mit anderen Trägern sozialer Sicherung. Sie nimmt insbesondere die Aufgaben nach der Datenerfassungsverordnung (DEVO) und der Datenübermittlungsverordnung (DÜVO) wahr, d. h. an sie senden die zuständigen Stellen die Versicherungsdaten aller Rentenversicherten, von ihr werden sie auf die zuständigen Rentenversicherer und die Bundesanstalt für Arbeit verteilt. Sie kontrolliert auch, ob Versicherungsnummern mehrfach vergeben sind. Die Gewährleistung des Datenschutzes im System der sozialen Sicherung wird durch eine Reihe von Faktoren bestimmt:

a) Dieser ohnehin schon stark automatisierte Bereich steht vor einer grundlegenden technologischen Umstellung. Die vorhandenen Datenverarbeitungssysteme werden in absehbarer Zeit durch wesentlich vielseitiger nutzbare Informationssysteme abgelöst werden. Derartige Informationssysteme werden z. B. in folgenden Bereichen entwickelt:

   — Die Bundesanstalt für Arbeit plant, das Arbeitsvermittlungsverfahren zu automatisieren.

   — Die Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (Essen) hat ein Grobkonzept für das System DVDIS: „Datenerfassung, Verarbeitung, Dokumentation und Informationsverbund in den sozialärztlichen Diensten mit Hilfe der elektronischen Datenverarbeitung" erarbeitet (vgl. das Gutachten von A. Podlech, Datenschutzprobleme einer Dokumentation im Vertrauensärztlichen Dienst und der gemeinsamen Forschung im Bereich der gesetzlichen Sozialversicherung, München 1978). Hinter diesem Titel steht offenbar das Vorhaben, eine personenbezogene Dokumentation aufzubauen, in der die medizinischen Daten (Krankheitsverläufe, Rehabilitationsmaßnahmen) aus der Renten- und Krankenversicherung (später möglicherweise unter Einschluß der Bundesanstalt für Arbeit und der betriebsärztlichen Dienste) zusammengeführt werden und bei Bedarf anderen Stellen zur Verfügung stehen sollen.

   — Der Bundesverband der Betriebskrankenkassen plant ein Informationssystem der Betriebskrankenkassen (ISBKK), das die etwa 800 Betriebskrankenkassen in einem Datenfernverarbeitungsnetz zusammenschließen soll.

   — Ein Verbund von dezentralen Subsystemen ist auch für den Bereich der Ortskrankenkassen im Aufbau („Informations- und Datenverarbeitungssystem für die Ortskrankenkassen", IDVS/OKK). Realisiert sind bisher die Anwendungen Mitgliederbestandsführung, Beitragswesen und Finanzwesen. Die zentral entwickelte Software wird bereits in zehn Rechenzentren eingesetzt. Die Ausweitung auf alle Rechenzentren soll voraussichtlich im Jahre 1980 abgeschlossen sein.

   — Der Hauptverband der gewerblichen Berufsgenossenschaften plant ein zentrales Informationssystem, an dem die gewerblichen Berufsgenossenschaften, die landwirtschaftlichen Berufsgenossenschaften und die Gemeindeunfallversicherungsträger beteiligt werden sollen.

   — Die Bau-Berufsgenossenschaften entwickeln ein arbeitsmedizinisches Informationssystem.

   Ich werde mit Nachdruck dafür eintreten, daß die vorgenannten und andere, hier nicht erwähnte Projekte von Anfang an den Belangen des Datenschutzes Rechnung tragen.

b) Überlegungen zur Fortentwicklung des Gesundheitswesens, wie sie in den vorstehend beispielhaft aufgeführten Informationssystemen dokumentiert werden, dürfen sich nicht mit technischer Perfektion begnügen. Im Mittelpunkt der Bemühungen um das Gesundheitswesen muß der Mensch stehen. Unter dieses Ziel ist auch das unlängst verabschiedete „Programm der Bundesregierung zur Förderung von Forschung und Entwicklung im Dienste der Gesundheit 1978—1981"

zu stellen. Ich sehe es als meine besondere Aufgabe an — und hierin werde ich durch zahlreiche Gespräche mit Bürgern, mit Trägern der sozialen Sicherung und ihren Verbänden, mit Ärzten und ihren Zusammenschlüssen bestärkt —, mein Augenmerk vor allem darauf zu richten, daß das letzte Glied der Kette, nämlich der Versicherte, Patient und betroffene Bürger vor dem undurchdringlich scheinenden Geflecht von Institutionen und unterschiedlichen Interessen nicht auch zum schwächsten wird. Ich werde im Rahmen meiner Beratungsfunktion bei der Entwicklung der in der Planung befindlichen Informationssysteme darauf hinwirken, daß der Datenschutz innerhalb der Gesundheitspolitik das gebührende Gewicht erhält.

3.5.2 Eingaben von Bürgern

Die Anzahl von Eingaben von Bürgern aus den Bereichen der sozialen Sicherung und des Gesundheitswesens ist relativ gering. Es wäre jedoch voreilig, hieraus den Schluß zu ziehen, daß es insoweit keine Probleme gibt. Viel näher liegt die Annahme, daß die zuständigen Verwaltungen „geräuschlos" funktionieren und insoweit keine persönliche Betroffenheit offenbar wird.

In einer Vielzahl von Fällen haben sich Bürger gegen die ihrer Ansicht nach unberechtigte Verweigerung von Auskünften hinsichtlich ihrer medizinischen Daten gewandt. Ich habe diese Fälle mangels Zuständigkeit nicht weiterverfolgen können. Sie geben mir aber Anlaß zu der Sorge, daß das informationelle Selbstbestimmungsrecht der Patienten nicht immer hinreichend ernst genommen wird.

Einige Eingaben betrafen den Umfang des Auskunftsanspruchs gem. § 13 BDSG der Mitglieder gegenüber ihren Krankenkassen. Viele Kassen geben offenbar grundsätzlich keine Auskunft über Diagnosedaten, sondern verweisen die Mitglieder pauschal an die behandelnden Ärzte. Ich weise mit Nachdruck darauf hin, daß diese Praxis mit dem Gesetz nicht in Einklang steht. Auch wenn ich einräumen muß, daß die Mitarbeiter der Kassen hier in kaum lösbare Konflikte kommen können — ich denke etwa daran, daß das Mitglied unheilbar an Krebs erkrankt ist —, so erwarte ich doch von den Kassen und ihren Verbänden ein Auskunfts*verfahren,* das den berechtigten Belangen der betroffenen Bürger besser gerecht wird. Eine Lösung könnte darin bestehen, daß die Kasse einen bestimmten Arzt mit der Erteilung der Auskünfte aus ihren Dateien beauftragt.

Eine Reihe von Eingaben betrifft ärztliche Gutachten in der Arbeitsverwaltung. Für die Bürger ist es schwer einsehbar, daß ihnen bezüglich dieser Gutachten, die zum Beispiel das Schicksal eines Arbeitslosen maßgeblich bestimmen können, keine Auskunftsrechte nach § 13 BDSG zustehen. Meine Prüfungen, ob es sich bei diesen Gutachten um Bestandteile von Dateien handelt, laufen noch. Soweit das nicht der Fall ist, werde ich darauf achten, daß ein Akteneinsichtsrecht, wie es das Verwaltungsverfahrensgesetz bereits vorsieht, auch im X. Buch des Sozialgesetzbuches, dessen Entwurf eine entsprechende Bestimmung enthält, verankert wird.

Viele Bürger und Ärzte haben sich besorgt über den Umgang speziell mit psychiatrischen Gutachten gezeigt. Auch wenn ich bis jetzt keine Hinweise auf absichtlichen Mißbrauch habe, so dürfte doch die Praxis in vielen Bereichen noch verbesserungsfähig sein. Die folgende Eingabe möge das verdeutlichen: Ein Lehrer war 1968 hauptsächlich wegen einer psychischen Erkrankung aus dem Schuldienst ausgeschieden. Inzwischen hat er sich in verschiedenen Berufen bewährt und wünscht, erneut als Lehrer zu arbeiten. Bei verschiedenen Bewerbungen mußte er jedoch feststellen, daß seine Personalakte ein ärztliches Gutachten enthält, das einen Zustand von 1968 beschreibt und ihm damit die faire Chance einer Neueinstellung nimmt, weil sein jetziger Gesundheitszustand aus der Akte nicht ersichtlich ist. Der zuständige Landesdatenschutzbeauftragte ist im Sinne des Petenten mit Erfolg tätig geworden.

Ich werde darauf hinwirken, daß insbesondere psychiatrische Gutachten nicht wie andere Bestandteile von (Personal-)Akten behandelt, sondern in besonderer Weise gesichert und getrennt aufbewahrt werden, so daß der Zugang zur Akte nicht automatisch die Einsichtsmöglichkeit in derartige Gutachten eröffnet.

3.5.3 Überprüfungen gemäß § 19 Abs. 1 BDSG

3.5.3.1 Vorgehensweise

In der Aufbauphase meines Amtes ging es vor allem darum, den Stand der Datenverarbeitung im Bereich der sozialen Sicherung durch praktische Anschauung kennenzulernen und mir einen Überblick über die Umsetzung des Datenschutzes zu verschaffen. Die tatsächliche Auswahl der besuchten bundesunmittelbaren Körperschaften des öffentlichen Rechts war so auch durch Zufälle bedingt. Daher möchte ich in diesem Bericht davon absehen, die Körperschaften namentlich zu benennen, obwohl zum Teil gravierende Mängel festgestellt wurden.

Der BfD hat im Jahre 1978 folgende Überprüfungen vorgenommen:

- bei einer kleineren Berufsgenossenschaft,
- bei einer großen Ersatzkasse mit zwei Geschäftsstellen in verschiedenen Städten,
- bei einer Geschäftsstelle einer anderen großen Ersatzkasse,
- bei einer großen Betriebskrankenkasse sowie zwei ihrer Geschäftsstellen in einer Stadt.

Die Kontrollen zur Einhaltung der Datenschutzvorschriften hatten bisher nicht so sehr den Charakter von Prüfungen als vielmehr den von Informations- und Beratungsbesuchen. Gemeinsam mit den Anwendern sollten Schwachstellen gefunden und alternative Lösungsansätze erarbeitet werden. Ziel dieses Verfahrens ist es, den Anwendern durch fachliche Beratung bei der Entwicklung eines Datenschutzsystems behilflich zu sein.

Um hierfür möglichst rasch einen Überblick über den Aufbau und die Ablauforganisation der besuchten Stellen zu gewinnen, werden als Einstieg der interne Datenkatalog gemäß § 15 BDSG sowie das Verzeichnis der Anwendungsgebiete benutzt. Auf diese Weise sind kritische Verfahren leicht auszumachen. Ein Gesamtbild des Standes der Datenverarbeitung bei der besuchten Stelle ergibt sich regelmäßig aus einer Analyse der Vorschriften für die Softwareentwicklung, einem Überblick über den Rechenzentrumsbetrieb und der Programmdokumentation.

Das Prüfteam besteht vorerst aus zwei Mitarbeitern — einem Juristen und einem DV-Spezialisten —. Sein Hauptgesprächspartner ist der interne Datenschutzbeauftragte. Er vermittelt die Kontakte zur Geschäftsleitung, zu den Fachabteilungen, dem Personalrat, dem Rechenzentrum usw.

Zum Abschluß des in der Regel einwöchigen Besuchs wird mit der Geschäftsleitung ein Gespräch geführt, in dem Stärken und Schwächen des jeweiligen Datenschutz-Systems besprochen werden.

Die wesentlichen Ergebnisse dieses Gesprächs werden der besuchten Stelle in einem zusammenfassenden Schreiben noch einmal mitgeteilt.

Dieses auf der Kooperationsbereitschaft der Anwender aufbauende Konzept hat sich bisher bewährt. Ob es sich in jedem Fall auch in der Zukunft aufrechterhalten läßt, kann erst nach weiteren Erfahrungen beurteilt werden.

3.5.3.2 Ergebnisse

— Besuch einer Berufsgenossenschaft

Der Besuch einer Berufsgenossenschaft mit einem kleineren Rechenzentrum und weniger als zehn Mitarbeitern in der Datenverarbeitung hat deutlich gemacht, daß es für derartige Anwender schwierig und mit den gegenwärtig überwiegend genutzten Technologien fast unmöglich ist, allen Datenschutz- bzw. Datensicherungsanforderungen zu genügen. Im einzelnen wurden folgende Mängel festgestellt:

- Formulare und Fragebögen waren noch nicht entsprechend dem § 9 Abs. 2 BDSG umgestellt.
- Der interne Datenkatolog (§ 15 BDSG) war noch nicht vollständig; insbesondere fehlten manuelle Dateien in der Bestandsaufnahme.
- Das Datensicherungskonzept muß neu durchdacht werden:
  - Der Objektschutz des Bandarchivs war noch unzureichend.
  - Das Vieraugenprinzip im Rechenzentrum war nicht immer gewährleistet.
  - Rechenzentrum und Bandarchiv waren nicht voneinander getrennt.
  - Die Funktionstrennung zwischen Arbeitsvorbereitung, Programmierung usw. war nicht gewährleistet.

Die Berufsgenossenschaft zeigte ein erfreulich hohes Problembewußtsein und große Bereitschaft, die festgestellten Mängel im Rahmen ihrer begrenzten Ressourcen zu beseitigen.

— Besuch einer großen Ersatzkasse

Wie nicht anders zu erwarten, hatte die Kasse als großer und finanzkräftiger Anwender ein teilweise vorbildliches Datensicherungskonzept vorzuweisen. Unzureichend war jedoch der Objektschutz: Das Rechenzentrum der Kasse liegt praktisch zu ebener Erde, ist von zwei Seiten verglast und weder durch Panzerglas, Vergitterung noch durch irgendeine Alarmvorrichtung gesichert. Im Rechenzentrum werden sämtliche Stammdaten der Mitglieder auf Platte bereitgehalten. Das Bandarchiv dieser Kasse ist für einen kriminellen Dritten leicht zugänglich. Im Gegensatz zur im ganzen erfreulichen Datensicherungspraxis steht die Behandlung der Leistungsdaten. Diese einschließlich der ärztlichen Diagnosen werden auf Leistungskarten festgehalten. Die Karten befinden sich in Karteien der einzelnen Geschäftsstellen in unverschlossenen Schubfächern und stehen dem Sachbearbeiter der Kasse offen zur Verfügung. Die Kasse hat sich hierzu auf den Standpunkt gestellt, bei diesen Karteien handele es sich nicht um Dateien im Sinne des Gesetzes. Diese Auffassung ist unhaltbar und wird auch von anderen Krankenkassen nicht geteilt. Der Standpunkt der Kasse ist deshalb so bedauerlich, weil er die Entstehung des Bewußtseins von der besonderen Sensibilität der Diagnosedaten verhindert.

Im übrigen war bei dieser Kasse das Auskunftsverfahren gemäß § 13 BDSG zu beanstanden. Sie gibt lediglich — insofern konsequent — Auskunft über die automatisch geführten Bestandsdaten. Daß sie verpflichtet ist, eine vollständige Auskunft zu geben, war ihr nicht bewußt.

Der Besuch dieser Kasse hat gezeigt, daß organisatorische Größe und entwickelter Datenschutz nicht zusammenfallen müssen.

— Besuch der Geschäftsstelle einer anderen großen Ersatzkasse

Der Eindruck, den ich hinsichtlich der Verwaltung der Leistungsdaten bei der vorstehend genannten Kasse gewonnen habe, hat sich auch hier bestätigt. Die Leistungskarten mit ihren höchst sensiblen diagnostischen Details werden in nicht besonders gesicherten Aktenschränken aufbewahrt. Die gewonnenen Erkenntnisse lassen befürchten, daß die Leistungsdaten bei den meisten Kassen nicht ihrer Bedeutung entsprechend gesichert sind. Die Kassen sind aufgefordert, hier für Abhilfe zu sorgen.

Die erwähnte Ersatzkasse praktiziert das Auskunftsverfahren nach § 13 BDSG, indem sie Fotokopien der Vorderseite der Leistungskarten versendet. Auf mein Einschreiten hin wird sie in Zukunft in einem noch zu präzisierenden Verfahren auch die Diagnosedaten auf der Rückseite dieser Leistungskarte dem Auskunftsberechtigten zugänglich machen.

— Besuch einer großen Betriebskrankenkasse

Die Kasse hat keinen Datenschutzbeauftragten bestellt; Belange des Datenschutzes werden dort vom Leiter der Abteilung DV-Verfahren mit wahrgenommen. Diese Lösung erscheint in diesem konkreten Fall vertretbar. Die Problematik der Leistungsdatenverwaltung stellt sich bei dieser Betriebskrankenkasse insofern anders, als die Geschäftsstellen in die Betriebsgebäude integriert sind und somit von einem funktionsfähigen Werkschutz mitbewacht werden. Überdies waren die Leistungskarten in beiden besuchten Geschäftsstellen in verschließbaren Schränken aufbewahrt. Zu beanstanden war bei dieser Kasse der interne Datenkatalog gemäß § 15 Satz 2 Nr. 1 BDSG, der für Dritte keinen zusammenhängenden Überblick über die Datenverarbeitung gewinnen ließ. Die Kasse wird bis Ende März 1979 den erforderlichen Datenkatalog aufstellen.

Als einzige der besuchten hatte diese Körperschaft sich schon frühzeitig einen Überblick über Informationsbewegungen aus manuellen Dateien verschafft.

3.5.3.3 Weitere Erkenntnisse, Gesamteindruck

Am Rande der Prüfungen habe ich erfahren, daß Mitarbeiter zweier Ersatzkassen Listen mit den Stammdaten von jeweils etwa 100 000 Versicherten entwendet und zum Verkauf angeboten haben. Allerdings handelte es sich in diesen Fällen nicht um Leistungs- und Diagnosedaten. Die Entstehung eines größeren Schadens konnte rechtzeitig abgewendet werden. Diese Fälle zeigen aber hinlänglich, daß auch dort, wo traditionell mit empfindlichem Datenmaterial umgegangen wird, Lücken im Datenschutzsystem anzutreffen sind. Daher muß das Problembewußtsein weiter geschärft werden. Im übrigen zeigt sich deutlich, daß das Datenschutzbewußtsein der Datenverarbeiter größer ist, als allgemein angenommen wird. Es war in allen Fällen ausgeprägter als das der übrigen Mitarbeiter, in einem Fall sogar deutlich besser als das des internen Datenschutzbeauftragten.

3.5.4 Einzelne Aktivitäten und Datenschutzprobleme

3.5.4.1 Datenabgleich zur Durchführung des Bundeskindergeldgesetzes

Mehrere Landesministerien haben mich gefragt, in welcher Weise der Datenabgleich zwischen der Bundesanstalt für Arbeit (BA) und den Meldebehörden zur Durchführung des Bundeskindergeldgesetzes (BKGG) erfolgen soll. Ich spreche mich grundsätzlich dafür aus, diesen Abgleich bei den Meldebehörden vorzunehmen, und zwar aus folgenden Erwägungen:

Kindergeld wird allgemein — wenn auch nicht ausnahmslos — bis zum 18. Lebensjahr eines Kindes gewährt. Volljährige Kinder werden bis zum 27. Lebensjahr berücksichtigt, wenn sie sich in Schul- oder Berufsausbildung befinden, ein freiwilliges soziales Jahr leisten oder unter besonderen Voraussetzungen den Haushalt des Kindergeldberechtigten führen. In Einzelfällen kann Kindergeld auch über das 27. Lebensjahr hinaus gezahlt werden. Wegen der Einzelheiten sei auf die gesetzlichen Vorschriften verwiesen.

Aus den Regelungen des BKGG ergibt sich, daß *in keiner Altersgruppe alle Kinder* einen Anspruch auf Kindergeld begründen, sondern daß jeweils die tatbestandlichen Voraussetzungen für das Bestehen eines Anspruchs geprüft werden müssen. Es bereitet der BA verhältnismäßig geringen Aufwand, aus den gespeicherten Datenbeständen diejenigen Daten auszuwählen, als Duplikat herzustellen und an die jeweils zuständigen Landesbehörden zu übermitteln, die für die Gewährung von Kindergeld anspruchsbegründend sind. Wenn der Abgleich bei der BA erfolgte, müßten die Meldebehörden der BA Daten aller bei ihnen registrierten Kinder sogar über das 27. Lebensjahr hinaus und von deren Eltern mitteilen. Damit würden auch Personen betroffen, für die kein Anspruch auf Kindergeld besteht oder die keinen Antrag darauf stellen wollen. Der BA würden somit mehr Daten übermittelt, als für ihre Aufgabenerfüllung notwendig ist.

Bei dem hier vorgeschlagenen Verfahren, die Daten von der BA an die Meldebehörden zu übermitteln, würde zwar das personenbezogene Datum „Kindergeldberechtigung" den Meldebehörden zur Kenntnis gelangen. Seine Mitteilung beruht aber auf einem Antrag, den der Kindergeldberechtigte gestellt hat. Zur Begründung dieses Antrags hat der Antragsteller alle für die beantragte Leistung erheblichen Tatsachen anzugeben und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte — hier also die Meldebehörde — zuzustimmen oder Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen (§ 60 SGB I; s. Hauck/Haines, SGB I, K § 60 Rdnr. 12). Die Pflichten des Antragstellers gemäß § 60 Abs. 1 SGB I müssen ihm bei der Antragstellung durch geeignete Formulargestaltung verdeutlicht werden. Denn es sind Fälle denkbar, in denen der Antragsteller zwar das Kindergeld erhalten möchte, aber nicht damit einverstanden ist, daß die BA die Tatsache der Kindergeldberechtigung, die dem Sozialgeheimnis unterliegt, der Meldebehörde mitteilt. In einem solchen Fall muß es dem Antragsteller ermöglicht werden, selbst Beweisurkunden zu beschaffen und vorzulegen, ohne daß er dabei das personenbezogene Datum „Kindergeldempfänger" gegenüber der Meldebehörde offenbart. Diese Fälle sind dann von dem Abgleich der Datenbestände auszunehmen.

3.5.4.2 Durchbrechungen des Sozialgeheimnisses

Da der BfD nicht nur die Einhaltung der Vorschriften des BDSG, sondern auch die Einhaltung anderer Vorschriften über den Datenschutz — vgl. die beispielhafte Aufzählung in § 45 BDSG — zu kontrollieren hat, galt besondere Aufmerksamkeit dem in der Öffentlichkeit viel diskutierten Sozialgeheimnis. Dieses wird durch § 35 SGB I — eine „andere Vorschrift über den Datenschutz" im Sinne des § 19 Abs. 1 BDSG — geschützt. In zahlreichen Fällen war aber festzustellen, daß in der Praxis erhebliche Unsicherheiten im Umgang mit dieser Vorschrift

bestehen. Sie führen dazu, daß einige Träger der Sozialversicherung nur in eng begrenzten Ausnahmefällen Daten an Dritte übermitteln, während andere Träger deutlich großzügiger verfahren. Insbesondere geht es um die Übermittlung von Namen und Anschriften des Versicherten und der Namen und Anschriften gegenwärtiger oder früherer Arbeitgeber. Nach derartigen Informationen fragen namentlich Strafverfolgungs- und Verfassungsschutzbehörden.

In Pressemeldungen wurde wiederholt der Vorwurf erhoben, es erfolge ein Datenabgleich zwischen dem Bundeskriminalamt und den Rentenversicherungsträgern. Die daraufhin von mir angestellten Ermittlungen haben ergeben, daß die Träger der gesetzlichen Rentenversicherung lediglich in *konkreten Einzelfällen* Amtshilfeersuchen bearbeiten. Soweit derartige Ersuchen statt bei der jeweiligen Versicherungsanstalt beim Verband Deutscher Rentenversicherungsträger e. V. (VDR) eingehen, werden sie dort nach den Beschlüssen seiner zuständigen Fachausschüsse behandelt. Dabei wurde in der Vergangenheit der aktuelle Kontoführer, d. h., derjenige Versicherungsträger, der im Zeitpunkt des Eingangs des Amtshilfeersuchens das Versicherungskonto der betroffenen Person führte, ermittelt, das Amtshilfeersuchen an den Kontoführer zur Erledigung abgegeben und der anfragenden Stelle Abgabenachricht erteilt. Lediglich in einem Fall wurde im Zusammenhang mit der Terroristenfahndung im Jahre 1975 von dem vorstehend geschilderten Einzelfallverfahren abgewichen und nach Einschaltung der zuständigen Bundesressorts auf eine Vielzahl von Anfragen — es handelte sich um mehrere tausend Namen, die auf einem Magnetband des Bundeskriminalamtes an den VDR übermittelt wurden — eine Vielzahl von Antworten erteilt. Auch in diesem einzigen Ausnahmefall wurden jedoch keine Anschriften mitgeteilt, sondern lediglich Hinweise auf den (die) Rentenversicherungsträger gegeben, bei dem (denen) die Anschrift der gesuchten Person *möglicherweise* erfragt werden könne.

Seit Inkrafttreten des BDSG ist der VDR dazu übergegangen, Amtshilfeersuchen urschriftlich mit einem Standardschreiben an den jeweils für das aktuelle Konto zuständigen Versicherungsträger abzugeben. Eine Abgabenachricht wird nicht mehr erteilt, so daß die anfragende Stelle vom VDR weder erfährt, ob die betreffende Person überhaupt ein Versicherungskonto in der deutschen gesetzlichen Rentenversicherung besitzt, noch wer gegebenenfalls der aktuelle Kontoführer für dieses Konto ist. Die Entscheidung, ob und wie die einzelnen Amtshilfeersuchen beantwortet werden, liegt nunmehr also ausschließlich bei dem zuständigen Rentenversicherungsträger. Sie ist nach § 35 SGB I zu treffen.

Das Sozialgeheimnis ist die Grundlage der Vertrauensbeziehungen zwischen den betroffenen Bürgern und den Leistungsträgern der sozialen Sicherung. Es soll garantieren, daß jeder zum Arzt, ins Krankenhaus oder zu einer Sozialbehörde gehen kann, ohne befürchten zu müssen, daß diese Tatsache Außenstehenden bekannt wird oder daß ihm daraus Nachteile entstehen. Auch die Sozialleistungsträger betonen zu Recht, daß alle personenbezogenen Daten, die ihnen anvertraut sind, streng abgeschirmt werden müssen. Unsicherheiten bei der praktischen Handhabung des § 35 SGB I müssen so schnell wie möglich ausgeräumt werden. Ich setze mich daher mit Nachdruck dafür ein, daß § 35 SGB I um einen abschließenden Katalog der Fälle befugter Offenbarung ergänzt wird. Die einzelnen Offenbarungsbefugnisse müssen als Ausnahmetatbestände eng formuliert werden und dürfen das Geheimhaltungsgebot nicht durch generalklauselartige Wendungen wieder aufweichen. Das nötigt zu Differenzierungen nach Datenarten und Regelungsgegenständen, z. B. Planung, Forschung, Strafverfolgung, Sicherung gesetzlicher Unterhaltspflichten.

3.5.4.3 Ersatzkassen als Wettbewerbsunternehmen?

Es ist behauptet worden, Ersatzkassen seien Wettbewerbsunternehmen im Sinne des § 7 Abs. 1 Satz 2 und Absatz 2 Satz 2, § 22 Abs. 1 Satz 2 und § 31 Abs. 1 Satz 1 BDSG. Davon hängt ab, ob statt gewisser Vorschriften des Zweiten Abschnitts des BDSG, die auf die Datenverarbeitung bei Behörden und anderen öffentlichen Stellen zugeschnitten sind, Vorschriften des Dritten (oder Vierten) Abschnitts anzuwenden sind, die für die Datenverarbeitung bei nicht-öffentlichen Stellen gelten. Ich bin der Ansicht daß Ersatzkassen nicht als Wettbewerbsunternehmen anzusehen sind.

Die Rechtsordnung kennt keinen allgemein verbindlichen Begriff des „Wettbewerbs" oder des „Unternehmens, das am Wettbewerb teilnimmt". Was Wettbewerb ist, beurteilt sich nach dem jeweiligen Regelungsgegenstand und den Zusammenhängen, in denen dieser steht. Das gilt etwa für den „unlauteren Wettbewerb" im Sinne des Gesetzes gegen den unlauteren Wettbewerb, für den Wettbewerb im Sinne des Gesetzes gegen Wettbewerbsbeschränkungen, aber auch für den Begriff des „Unternehmens, das am Wettbewerb teilnimmt", im Sinne des BDSG.

Wettbewerb in einem allgemeinen Sinne liegt vor, wenn mehrere Unternehmen ihre auf Geschäftsabschlüsse mit Dritten gerichteten Entscheidungen gemäß der jeweiligen Marktlage selbständig treffen und durchführen, ohne in ihrem Verhalten mehr beschränkt zu sein, als sich aus dem gleichfalls selbständigen Verhalten anderer Unternehmen ergibt, die auf einem bestimmten Markt gleiche Ziele verfolgen.

Folgt man dieser Definition, so ist es zumindest zweifelhaft, ob eine Ersatzkasse an einem Wettbewerb teilnehmen kann, denn sie wird durch gesetzliche Vorschriften in ihrem Verhalten erheblich beschränkt:

Gehört ein Versicherungspflichtiger zu dem Personenkreis, für den die Ersatzkasse errichtet ist, so darf sie ihm grundsätzlich den Beitritt nicht versagen, insbesondere nicht von seinem Lebensalter oder seinem Gesundheitszustand abhängig machen (§ 505 Abs. 1 RVO). Kraft Gesetzes gehören zu ihren Mitgliedern bestimmte Rentner und Behinderte (§ 514 Abs. 2 i. V. m. § 257 a und c RVO) wie auch Arbeitslose (§ 159 AFG). Hinzu kommen weitere,

die Entscheidungsfreiheit der Ersatzkassen erheblich einschränkende Vorschriften über die Gestaltung der Beiträge (§ 514 Abs. 3 i. V. m. § 385 Abs. 1 RVO) sowie darüber, welche Leistungen zu gewähren sind und welche gewährt werden dürfen (§§ 507, 508 RVO).

Versteht man unter Wettbewerb das freie Anbieten von Leistungen durch Konkurrenten zu gleichen oder vergleichbaren Bedingungen an denselben Personenkreis, so sind Fälle eines Wettbewerbs zwischen einer Ersatzkasse und einem anderen Träger der gesetzlichen Krankenversicherung — einer anderen Ersatzkasse wie auch einer der in § 225 RVO genannten Kassen (RVO-Kassen) — möglich. Auch zwischen einer Ersatzkasse und einer privaten Krankenversicherung kann ein Wettbewerb in diesem Sinne stattfinden. Allerdings ist der Personenkreis, um den geworben wird, verschieden, je nachdem, wer mit wem konkurriert: Ersatzkassen sind für verschiedene berufsbezogene Personenkreise errichtet worden, die sich teilweise überschneiden. Bei den Versicherungsunternehmen des privaten Rechts finden sich ebenfalls Spezialisierungen auf bestimmte Berufsgruppen. Bei den RVO-Kassen ergeben sich Begrenzungen der in Betracht kommenden Personenkreise daraus, daß sie Orts-, Betriebs- oder Innungskrankenkassen sind. Bei den Mitteln, mit denen konkurriert wird, kann es sich um Leistungen und Beitragssätze handeln, aber auch um besondere Serviceangebote.

Zweck der Ausnahmeregelung ist es, Wettbewerbsverzerrungen zu vermeiden. Durch die Anwendung der Vorschriften des Zweiten Abschnitts auf die Ersatzkassen könnte eine Wettbewerbsverzerrung im Verhältnis zu anderen Trägern der gesetzlichen Krankenversicherung schon deshalb nicht eintreten, weil auch diese, soweit das BDSG überhaupt für sie gilt, den Vorschriften des Zweiten Abschnitts unterworfen sind. Für private Krankenversicherungen gelten zwar nicht die Vorschriften des Zweiten, sondern die des Dritten (oder Vierten) Abschnitts des BDSG. Für das Verhältnis der Ersatzkassen zu ihnen ist aber zu berücksichtigen, daß der Wettbewerb, wenn man einen solchen überhaupt als gegeben ansieht, durch die genannten gesetzlichen Vorschriften, welche die Entscheidungsfreiheit der Ersatzkassen erheblich einschränken, ohnehin schon so verzerrt ist, daß demgegenüber eine weitere Verzerrung, die etwa durch Anwendung verschiedener Datenschutzvorschriften eintreten könnte, kaum mehr in Gewicht fallen kann.

Hinzu kommt, daß sich die Ersatzkassen allenfalls mit einem kleinen Teil ihrer Aktivitäten auf einen Wettbewerb mit privaten Krankenversicherern einlassen können. Mit dem weitaus überwiegenden Teil ihrer Tätigkeit treten die Ersatzkassen als Träger öffentlicher Verwaltung auf, die gesetzliche Aufgaben zu erfüllen haben, nicht als Unternehmen, die am Wettbewerb teilnehmen. Soweit sie überhaupt Aktivitäten entfalten, die man als Wettbewerb mit privaten Krankenversicherern verstehen könnte, handelt es sich lediglich um Randerscheinungen.

3.6 Wirtschafts- und Verkehrsverwaltung

Entsprechend den unterschiedlichen Zuständigkeiten des Bundes werden in den einzelnen Teilbereichen der Wirtschafts- und Verkehrsverwaltung personenbezogene Daten in sehr verschiedener Intensität verarbeitet. Gebieten mit massenhaftem Verwaltungsvollzug und entsprechend umfangreicher Verarbeitung personenbezogener Daten, wie der Post und dem Verkehrswesen, stehen Bereiche mit vorwiegend planender und kontrollierender Tätigkeit gegenüber, etwa Wirtschafts- und Landwirtschaftsverwaltung, wo personenbezogene Daten nur am Rande eine Rolle spielen. Dementsprechend wurden auch die Akzente in meiner Prüfungstätigkeit gesetzt.

3.6.1 Wirtschaftsverwaltung

Hier gab es nur wenige Eingaben und Anfragen. Erkenntnisse, die auch für andere öffentliche Stellen von Bedeutung sein dürften, ergaben sich bei folgendem Vorgang: Ein Bürger, dem ein Meinungsforschungsinstitut einen Fragebogen zugeschickt hatte, rief mich an, weil ihm aufgefallen war, daß dabei ein maschinell gedruckter Adreßaufkleber verwendet wurde, den sonst das Bundesministerium für wirtschaftliche Zusammenarbeit beim Vertrieb seiner Informationsschriften benutzte. Es stellte sich heraus, daß das Ministerium dem Diakonischen Werk Bayern, einem eingetragenen Verein, auf Wunsch eines kirchlichen Arbeitskreises etwa 7 000 Anschriften von Beziehern seines Pressespiegels zur Verfügung gestellt hatte, um eine Repräsentativerhebung über den entwicklungspolitischen Buchmarkt zu unterstützen, an deren Ergebnissen es auch selbst interessiert war. Die Angaben stammten aus Bestellformularen, mit denen jedermann um kostenlose Zusendung verschiedener Publikationsserien des Ministeriums bitten kann. In den Formularen wird auch nach der Zugehörigkeit zu bestimmten Gruppen oder Bereichen gefragt, etwa „Kirchen" oder „Gewerkschaften"; die vom Besteller anzukreuzende Schlüsselzahl ist auch als Kopfzeile in der Computer-Adresse enthalten. Die Untersuchung wurde vom Diakonischen Werk Bayern mit Hilfe eines privaten Meinungsforschungsinstituts durchgeführt.

Das Ministerium hat auf den engen Zusammenhang der Erhebung mit seiner Aufgabe der Öffentlichkeitsarbeit verwiesen; außerdem hätten sich die Betroffenen als entwicklungspolitisch besonders interessiert gezeigt, so daß davon habe ausgegangen werden können, daß sie auch gegen die Erhebung nichts einzuwenden hätten. Die Evangelische Kirche hat sich darauf berufen, daß die Übermittlung entgegen dem äußeren Anschein nicht an den privatrechtlichen Verein, sondern an den kirchlichen Arbeitskreis erfolgt und daher nach § 10 Abs. 2 BDSG gerechtfertigt sei.

Demgegenüber habe ich klargestellt, daß es an der *Erforderlichkeit* der Übermittlung zur Erfüllung der Aufgaben des Ministeriums (§ 11 Satz 1, 1. Alternative) fehlt. „Erforderlichkeit" bedeutet, daß eine der Verwaltung übertragene Aufgabe ohne Über-

mittlung personenbezogener Daten nicht ordnungsgemäß erfüllt werden kann, etwa weil Auskünfte eingeholt und hierzu bestimmte Informationen mitgeteilt werden müssen. Nur insoweit muß das Interesse der Betroffenen zurücktreten. Die Öffentlichkeitsarbeit dient nicht unmittelbar der Erfüllung der eigentlichen Verwaltungsaufgaben, sondern hat nur unterstützende Funktion. Die Datenübermittlung an die Kirche stand den primären Aufgaben des Ministeriums noch ferner.

Spezielle Eingriffsermächtigungen zur Erfüllung solcher Hilfsaufgaben bestehen nicht. Da der Verwaltung hier nicht das Erreichen eines bestimmten Erfolges aufgegeben ist, sondern nur das Wirken in eine bestimmte Richtung, können die Interessen der betroffenen Dritten ohne ins Gewicht fallende Nachteile in der Weise berücksichtigt werden, daß um die Zustimmung zur Datenübermittlung gebeten wird. Auch auf die zweite Alternative des § 11 Abs. 1 BDSG kann die Übermittlung nicht gestützt werden, da die schutzwürdigen Belange der Betroffenen entgegenstanden. Sie brauchten es nicht hinzunehmen, daß ihre Zugehörigkeit zu bestimmten Personengruppen bekannt wurde.

Ob es zutrifft, daß die Daten nicht an die privatrechtliche Hilfsorganisation der Kirche, sondern unmittelbar an eine kirchliche Stelle übermittelt worden sind, braucht nachträglich nicht mehr geklärt zu werden. Für die Zukunft ist freilich klärungsbedürftig, inwieweit die Einbeziehung solcher Stellen in die privilegierende Vorschrift des § 10 Abs. 2 gerechtfertigt ist (vgl. auch unten 4.3).

Das Ministerium hat nach Bekanntwerden der Beschwerden sofort dafür gesorgt, daß die Betroffenen über die Verwendung ihrer Daten informiert wurden. Für die künftige Verwendung der Anschriftendatei wurden folgende Grundsätze festgelegt:

- Eine Übermittlung erfolgt nur noch, soweit die Betroffenen schriftlich eingewilligt haben.
- Die Empfänger der Adressen werden verpflichtet, die Betroffenen über die Herkunft der Daten und über den Zweck der Verwendung aufzuklären und die Daten nach der Durchführung des Vorhabens zu vernichten oder zurückzugeben.
- Die verschlüsselten Angaben in der Kopfleiste der Anschriften werden nicht mehr ausgedruckt.

Die Einhaltung dieser Regeln kann auch anderen öffentlichen Stellen, die Dateien über die Empfänger von Informationsmaterial führen, empfohlen werden.

3.6.2 Verkehrsverwaltung

3.6.2.1 Kraftfahrtbundesamt

Zahlreiche Beschwerden löste die Praxis der Verkehrsverwaltungen aus, die Angaben, die bei der An- und Ummeldung von Kraftfahrzeugen erhoben werden, Adressenverlagen für die Auswertung zu Werbezwecken zu überlassen. Zwar haben die für das Zulassungswesen zuständigen Landesverwaltungen in die Antragsformulare schon vor Jahren einen Passus aufgenommen, mit dem der Antragsteller erklären kann, ob er mit der Weiterleitung seiner Daten durch das Kraftfahrtbundesamt (das zur zentralen Bestandsführung Durchschriften aller Meldungen erhält) einverstanden ist. Meine Untersuchungen ergaben keine Hinweise auf vorsätzlichen Datenmißbrauch; ich habe jedoch festgestellt, daß das bisher geübte Verfahren eine Reihe von Mängeln aufweist, die dazu führen, daß in zahlreichen Fällen Daten ohne Einverständnis des Betroffenen übermittelt werden.

Viele Zulassungsämter verwenden Formulare, in denen auf den Text der Einverständniserklärung („Sind Sie einverstanden, daß das Kraftfahrtbundesamt ...") die Worte „Ja/Nein" folgen, jedoch kein Hinweis, ob die zutreffende Antwort gekennzeichnet oder die unzutreffende ausgestrichen werden soll. Dadurch kam es vor, daß Markierungen, die „Nein" bedeuten sollten, von der Behörde als „Ja" aufgefaßt wurden. Weitere Fehler ergaben sich dadurch, daß die Zulassungsämter auch die durch einen Bevollmächtigten, z. B. durch den Kraftfahrzeughändler, abgegebenen Erklärungen akzeptierten; den Betroffenen blieb dies jedoch regelmäßig unbekannt. Schließlich kam es vor, daß Ämter eine Zustimmung fälschlich als erteilt ansahen, wenn in der Erklärung weder „ja" noch „nein" angekreuzt war.

In den Beschwerdefällen habe ich veranlaßt, daß das Kraftfahrtbundesamt den Daten der Betroffenen umgehend einen Sperrvermerk beifügte und die Adressenverlage zur sofortigen Löschung der betreffenden Datensätze aufforderte (wozu diese sich vertraglich verpflichtet haben).

Zur Beseitigung der Mängel hat der Bundesminister für Verkehr in einer „Verlautbarung zur Erklärung des Fahrzeughalters über die Auswertung der Daten" (Verkehrsblatt Heft 20 vom 31. Oktober 1978) den Ländern empfohlen, die Einwilligung mit einer bestimmten Formulierung und unter Beachtung bestimmter Verfahrensgrundsätze einzuholen. Der vorgesehene Text stellt sicher, daß Inhalt und Umfang der Datenübermittlung so klar und unmißverständlich beschrieben werden, daß der Betroffene sich auf der Grundlage präziser Information frei entscheiden kann. Weiter wird klargestellt, daß es einer ausdrücklichen und vom Fahrzeughalter persönlich abgegebenen Einwilligung bedarf. Eine andere Person kann die Einwilligung nur erteilen, wenn sie dazu speziell und ausdrücklich bevollmächtigt ist.

Mit dem zentralen Bestandsverzeichnis der zugelassenen Kraftfahrzeuge und dem Verkehrszentralregister, in dem verkehrsrechtliche Entscheidungen von Behörden und Gerichten gespeichert werden, gehört das Kraftfahrtbundesamt innerhalb der Bundesverwaltung zu den bedeutendsten Verarbeitern personenbezogener Daten. Einen ersten Überblick über die dort bestehenden Probleme der Datenverarbeitung und des Datenschutzes habe ich mir bei einem Besuch an Ort und Stelle verschafft. Dabei hat sich herausgestellt, daß das große Volumen der Datenverarbeitung und die erhebliche Bedeutung der Speicherung und Übermittlung der Daten für die betroffenen Bürger tiefergehende Untersuchungen

erforderlich machen. Sie sollen im nächsten Jahr in Angriff genommen werden. Unabhängig davon habe ich meine Beratung in aktuellen Fragen, z. B. im Zusammenhang mit der Erweiterung des Rechenzentrums, angeboten.

3.6.2.2 Verkehrsunternehmen mit Bundesbeteiligung

In einer Eingabe beschwerte sich ein Bürger darüber, daß der Frankfurter Verkehrsverbund Dauerfahrausweise nur dann ausstellt, wenn zuvor ein „Bestellschein für eine FVV-Kundenkarte" ausgefüllt wird. In diesem Formular wird u. a. nach dem Geburtsdatum, nach der Sprache, nach der Ausbildung und nach dem Weg zur Starthaltestelle gefragt. Ein Hinweis auf die Freiwilligkeit dieser Angaben fehlt. § 9 Abs. 2 BDSG ist hier nicht anwendbar. Zwar erhalten die Fahrgäste die FVV-Kundenkarte bei der Fahrkartenausgabe der Bundesbahn oder bei den Verkaufsstellen der Stadtwerke Frankfurt a. M. Ein Vertrag kommt jedoch mit dem Frankfurter Verkehrsverbund GmbH zustande, an dem die Bundesbahn und die Stadtwerke je zur Hälfte beteiligt sind. Die Gesellschafter handeln insoweit im Namen der Gesellschaft. Daß das Beförderungsverhältnis dann wiederum mit einem der beteiligten Verkehrsträger — Bundesbahn oder Stadtwerke — zustande kommt, ändert daran nichts.

Ich würde es jedoch nicht für richtig halten, wenn Bürger, welche die Verkehrsleistungen der Bundesbahn in Anspruch nehmen, nur deshalb die in § 9 Abs. 2 BDSG vorgesehene Aufklärung nicht erhalten, weil sich die Bundesbahn in einem bestimmten Tarifgebiet mit einem anderen, ebenfalls öffentlich-rechtlichen Verkehrsträger zu einem Verbund zusammengeschlossen hat. Nach Abstimmung mit dem Hessischen Datenschutzbeauftragten und dem Regierungspräsidenten in Darmstadt als zuständiger Aufsichtsbehörde für den nichtöffentlichen Bereich habe ich deshalb angeregt, auf den Bestellformularen einen ausdrücklichen Hinweis auf die Freiwilligkeit derjenigen Angaben aufzudrucken, die für die Bearbeitung nicht zwingend erforderlich sind, auch wenn keine gesetzliche Bestimmung dieses verlangt.

3.6.3 Bundespost

Die Deutsche Bundespost zählt ebenso wie die Verkehrsverwaltung zu den Bereichen der Bundesverwaltung, in denen eine Fülle personenbezogener Daten verarbeitet wird. Es versteht sich daher von selbst, daß ich ihr meine besondere Aufmerksamkeit zuwende.

Ich habe festgestellt, daß das bisher verwendete Formular für die Anmeldung von Fernsprechanschlüssen nicht den Erfordernissen des BDSG entsprach. In den Formularen wurden u. a. die genaue Berufsangabe des Antragsstellers und eine Angabe zur überwiegenden Nutzung des Anschlusses erbeten. Neben diesen Fragen war am Rande des Formulars vermerkt „Angaben für Strukturuntersuchungen und Fernsprechbuchzwecke". Es war nicht deutlich gemacht, ob diese Informationen auf einer gesetzlichen Grundlage erhoben wurden oder freiwillig gemacht werden sollten. Dies wurde in mehreren an mich gerichteten Eingaben mit Recht bemängelt. Die Post hätte klarstellen müssen, daß diese Angaben freiwillig waren. Es wäre auch sinnvoll gewesen, in dem Formular anzugeben, daß diese Daten zu Untersuchungen über den künftigen Bedarf an Fernsprecheinrichtungen und für Werbezwecke der Postreklame verwendet werden. Auf meine Veranlassung wird z. Z. ein neues Formular entwickelt.

Die Übermittlung von Anschriften von Postkunden an die Postreklame GmbH zur Auswertung für Werbezwecke ist sowohl in der Datenschutzliteratur als auch vereinzelt von Betroffenen kritisch bewertet worden. Zugleich wurde gefordert, diese Daten nur mit ausdrücklicher Zustimmung des Betroffenen weiterzugeben.

Ich habe meine Untersuchungen in dieser Angelegenheit noch nicht vollständig abgeschlossen. Bis zu einer abschließenden Urteilsbildung wird zu berücksichtigen sein, daß die Bundespost ein eigenes Interesse daran hat, daß die werbende Wirtschaft ihre Kunden und sonstige Interessenten unter der richtigen Anschrift erreicht. Dies erspart der Post erhebliche Aufwendungen durch Nachsendungen. Dies allein vermag jedoch nicht als Rechtfertigung der gegenwärtigen Praxis zu dienen. Ich werde mich vielmehr dafür einsetzen, daß die an die Postreklame weiterzugebenden Daten auf diejenigen beschränkt werden, die auch sonst in Adreß- und Fernsprechbüchern enthalten sind. Geschieht dies, wird man nicht auf einem Einverständnis des Betroffenen in jedem Einzelfall bestehen müssen, sondern es als ausreichend betrachten können, wenn ihm die Möglichkeit gegeben wird, der Übermittlung an die Postreklame zu widersprechen. Damit wäre denjenigen, die sich durch die Übermittlung der Daten in ihren schutzwürdigen Belangen beeinträchtigt fühlen, geholfen. Damit keine Mißverständnisse entstehen: Diese Ausführungen beziehen sich nur auf den speziellen Fall, daß die Deutsche Bundespost Daten, die auch sonst in allgemein zugänglichen Quellen enthalten sind, an die werbende Wirtschaft übermittelt. Sie gelten nicht für die Übermittlung von Anschriften durch öffentliche Stellen an Private generell.

3.7 Nicht-öffentlicher Bereich

3.7.1 Voraussetzungen der Kontrolltätigkeit des Bundesbeauftragten

Die Anwendung des BDSG und anderer Vorschriften über den Datenschutz wirft im nicht-öffentlichen Bereich mindestens ebenso viele Probleme auf wie im öffentlichen. Im Berichtszeitraum zeigte sich dies an einer großen Zahl von Eingaben betroffener Bürger, aber auch an dem Wunsch vieler datenverarbeitender Stellen, mit mir über die bei ihnen aufgetretenen praktischen Fragen zu beraten, sowie an dem Interesse der Medien, gerade auch über diesen Bereich zu berichten.

Meine Möglichkeiten, gegenüber den verarbeitenden Stellen für einen wirksamen Datenschutz einzutreten, sind im nicht-öffentlichen Bereich begrenzt. Die Kontrollzuständigkeit liegt insoweit bei den Aufsichtsbehörden der Länder. Dennoch würde ich meine Aufgabe verkennen, wenn ich mich darauf beschränkte, die Eingaben und Anfragen an die jeweils örtlich zuständigen Aufsichtsbehörden weiterzuleiten. Das BDSG verwendet für den öffentlichen und den nicht-öffentlichen Bereich dieselben Grundbegriffe und trifft weithin dieselben oder ähnliche Regelungen. Um das vom Gesetzgeber erstrebte Ziel eines möglichst gleichwertigen Datenschutzes zu erreichen, bedarf es einer engen Kooperation mit den anderen für die Kontrolle des Datenschutzes zuständigen Stellen. Nicht zuletzt ist zu berücksichtigen, daß die für den nicht-öffentlichen Bereich geltenden Vorschriften des 3. und 4. Abschnittes auch im öffentlichen Bereich des Bundes zum Tragen kommen, nämlich insoweit, als es um die Tätigkeit öffentlich-rechtlicher Wettbewerbsunternehmen oder um die Verarbeitung personenbezogener Daten im Zusammenhang mit dienst- oder arbeitsrechtlichen Rechtsverhältnissen geht (vgl. § 7 Abs. 1 Satz 2 und Absatz 3 BDSG). Aus diesen Gründen ist ein intensiver Erfahrungsaustausch mit den obersten Aufsichtsbehörden für den Datenschutz der Länder aufgenommen worden. Dies entspricht der mir vom Gesetz übertragenen Aufgabe, auf eine Zusammenarbeiten mit allen Datenschutz-Kontrollinstitutionen hinzuwirken (§ 19 Abs. 5). Dank der Kooperationsbereitschaft der Länder, die schon früh ein Koordinierungsgremium, den sog. Düsseldorfer Kreis, geschaffen hatten, ist es bisher möglich gewesen und bestehen weiter gute Aussichten, den Datenschutz in nahezu allen wesentlichen Fragen einheitlich zu entwickeln.

3.7.2 Versicherungen

Eine große Anzahl von Beschwerden und Anfragen habe ich von Bürgern erhalten, denen von Versicherungsunternehmen formularmäßig — teils als Bestandteil des Versicherungsantrags, teils als getrennte Erklärung — eine sog. Datenschutzklausel zur Unterschrift vorgelegt worden war. Die Betroffenen wollten geklärt wissen, welche Konsequenzen ihre Unterschrift habe und ob das Verlangen der Versicherungsgesellschaften im Einklang mit den Datenschutzgesetzen stehe.

Die Klausel hat (mit geringen Variationen für die einzelnen Versicherungszweige) den folgenden einheitlichen Wortlaut:

> Ich ermächtige den Versicherer, die im Zusammenhang mit der beantragten Versicherung stehenden Daten zu speichern und an die betroffenen Rückversicherer, an die Versicherer der ... -Versicherungsgruppe und an andere Personenversicherer sowie an den ...-Verband zum gleichen Zweck zu übermitteln, soweit dies zur üblichen Betreuung des Ermächtigenden oder zur ordnungsgemäßen Durchführung der vertraglichen Beziehungen erforderlich ist. Gesundheitsdaten werden zu diesem Zweck nur an Personenversicherer und die betroffenen Rückversicherer weitergegeben. Die Vorschriften des Bundesdatenschutzgesetzes zur Datenübermittlung bleiben unberührt. Die Anschrift der jeweiligen Datenempfänger wird auf Wunsch mitgeteilt.

Nach Auffassung der Versicherungswirtschaft hat diese Klausel datenschutzrechtlich eine zweifache Bedeutung. Zum einen soll mit ihr die Benachrichtigungspflicht nach § 26 Abs. 1 BDSG erfüllt bzw. die dort alternativ geforderte Kenntnis „auf andere Weise" bewirkt werden. Zum zweiten soll in der Erklärung eine Einwilligung gemäß § 3 BDSG liegen, die dann praktische Bedeutung erlangt, wenn eine Übermittlung nicht durch § 24 BDSG oder durch eine andere Rechtsvorschrift gedeckt ist.

Unter beiden Gesichtspunkten bestehen jedoch Bedenken. Die in § 26 Abs. 1 BDSG vorgeschriebene Benachrichtigung obliegt der speichernden Stelle; sie soll dem Betroffenen die notwendige Information geben, damit dieser seine Kontrollrechte wahrnehmen kann. Auch eine „auf andere Weise" erlangte Kenntnis von der Speicherung macht eine Benachrichtigung deshalb nur dann entbehrlich, wenn sie die Bezeichnung der speichernden Stelle enthält. Es geht nicht an, daß die Mühe, im Einzelfall die speichernde Stelle ausfindig zu machen, auf die Betroffenen abgewälzt wird.

Das Bundesdatenschutzgesetz verlangt für die Verarbeitung personenbezogener Daten grundsätzlich die Einwilligung des Betroffenen. Eine freie Entscheidung hierüber setzt freilich ein Mindestmaß an Information voraus, welche Daten aus welchem Anlaß zu welchem Zweck an welche Empfänger übermittelt werden sollen. Aufgrund meiner Erfahrungen kann ich nicht bestätigen, daß die Klausel diesen Anforderungen entspricht.

Ich habe mich deshalb an die Datenschutz-Aufsichtsbehörden der Länder, denen der Großteil der Versicherungsunternehmen zugeordnet ist, gewandt und mich an den von diesen bereits eingeleiteten Verhandlungen mit der Versicherungswirtschaft beteiligt. Außerdem habe ich meine Vorstellungen dem Bundesaufsichtsamt für das Versicherungswesen nahegebracht, das im Hinblick auf seine Kompetenz zur Genehmigung der Datenschutzklausel (als Bestandteil des Geschäftsplans) ebenfalls an den Gesprächen mit der Versicherungswirtschaft beteiligt ist. Die gemeinsame Überzeugung der Datenschutzinstanzen geht dahin, daß eine Einwilligungsklausel aus der Sicht des Datenschutzes nur dann befriedigt, wenn den Betroffenen so klar, wie es angesichts der komplizierten Materie nur möglich ist, verdeutlicht wird, welches der Sinn und Zweck der verschiedenen vom Versicherer für nötig erachteten Übermittlungen ist — also z. B. Risikobeurteilung durch den Rückversicherer, vorbeugende Bekämpfung von Versicherungsbetrug mit Hilfe der Verbände, zentralisierte automatische Datenverarbeitung, Werbung und Beratung durch Schwester-Gesellschaften — und welche personenbezogenen Daten davon jeweils betroffen sind. Ein Höchstmaß an Information über das, was mit den Daten geschehen soll, dürfte auch hier das beste

Mittel sein, um unbegründetes Mißtrauen abzubauen.

3.7.3 Kreditsicherung

Ähnliche Probleme wie beim Informationsaustausch zwischen Versicherungen haben sich bei der Anwendung des BDSG auf den Austausch von Angaben über Kreditnehmer ergeben, der zwischen den Kreditinstituten (einschließlich der öffentlich-rechtlich organisierten) und anderen kreditgebenden Einrichtungen in großem Umfange stattfindet. Eine zentrale Rolle spielen dabei die Schutzgemeinschaften für allgemeine Kreditsicherung (Schufa), die in der sog. Bundes-Schufa zusammengeschlossen sind. Beim größten Teil aller Kredite bis zur Höhe von 30 000 DM, die von Privatpersonen in Anspruch genommen werden — z. B. beim Dispositionskredit der Banken, beim Teilzahlungskauf, aber auch schon bei Einräumung eines Kredits in Form einer Euro-Scheckkarte — werden Angaben über die Kreditvergabe sowie über den weiteren Geschäftsablauf an die Schufa gemeldet, die ihrerseits den angeschlossenen Unternehmen Auskünfte aus den ihr vorliegenden Daten erteilt, und zwar nicht nur auf Anfrage vor einer Kreditentscheidung, sondern auch durch Nachmeldungen über später eingetretene kreditrelevante Tatsachen. Zusätzliche Informationen werden aus allgemein zugänglichen Quellen, wie z. B. öffentlichen Registern (Schuldnerverzeichnis), bezogen.

In den Geschäftsbedingungen der Kreditinstitute findet sich hierzu die folgende zwischen dem Bundesverband deutscher Banken, dem Bundesverband der Deutschen Volksbanken und Raiffeisenbanken sowie dem Deutschen Sparkassen- und Giroverband abgestimmte Klausel:

> Im Zusammenhang mit der Aufnahme und Abwicklung dieses Darlehens werden der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) Daten über den Darlehensnehmer und etwaige Mitantragsteller zur Speicherung im Rahmen ihrer Tätigkeit übermittelt. Die Adresse der örtlich zuständigen Schufa wird ... auf Wunsch gern mitgeteilt; außerdem ist die Bundes-Schufa e. V., Kronprinzenstraße 28, 6200 Wiesbaden, zur Auskunftserteilung bereit.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, an die ich bei mir eingegangene Beschwerden weitergeleitet habe, haben den Verbänden mitgeteilt, daß die Übermittlung von Angaben aus Kreditverhältnissen durch § 24 BDSG nicht in allen Fällen gedeckt und daher eine Einwilligung der Betroffenen erforderlich sei. Die verwendete Klausel genüge jedoch nicht den Anforderungen des § 3 BDSG, da sie, insbesondere bei der Beschreibung des Datenumfangs, nicht konkret genug sei.

Die Verbände haben demgegenüber den Standpunkt bezogen, daß die Übermittlungen nach § 24 BDSG zulässig seien, da sie entweder im Rahmen der bestehenden Vertragsverhältnisse lägen oder durch die berechtigten Interessen der Unternehmen, denen gegenüber die schutzwürdigen Belange der Betroffenen zurückstehen müßten, gerechtfertigt seien. Die Klausel diene allein dem Zweck, den Betroffenen gem. § 34 Abs. 1 zweite Alternative BDSG über die Tatsache der Speicherung seiner Daten bei der Schufa in Kenntnis zu setzen.

Ich teile die Auffassung der Aufsichtsbehörden, daß ein genereller Informationsaustausch innerhalb der kreditgebenden Wirtschaft i. S. des § 24 Abs. 1 BDSG weder im Rahmen der Zweckbestimmung des Kreditverhältnisses mit dem Betroffenen liegt, noch das Interesse der Kreditwirtschaft, durch umfassenden Datenaustausch das Kreditrisiko zu minimieren, generell den schutzwürdigen Belangen des einzelnen vorgeht. Gegen einen solchen Vorrang spricht auch die Aussage der Verbände der Kreditwirtschaft, nach der ein Kreditinstitut aus Gründen des Bankgeheimnisses zur Weitergabe der Daten nicht berechtigt sei, wenn der Kunde widerspricht. Ich halte dieses Verfahren, das nach meiner Kenntnis in der Praxis eingehalten wird, auch unter dem Gesichtspunkt des Datenschutzes für geboten und würde es begrüßen, wenn bei den laufenden Verhandlungen zwischen den Verbänden der Kreditwirtschaft und den Aufsichtsbehörden für den Datenschutz eine entsprechende Übereinkunft erzielt würde.

3.7.4 Mitgliederdaten von Vereinigungen und Verbänden

In einigen Anfragen ging es um die Verwirklichung des Datenschutzes bei Vereinigungen und Verbänden. Zentral war dabei die Frage, unter welchen Voraussetzungen und in welchem Umfang personenbezogene Daten der Mitglieder Außenstehenden zugänglich gemacht werden dürfen. Hierüber herrscht weithin noch Unsicherheit.

Beispielsweise wurde angefragt, ob regionale Sportvereine berechtigt seien, Namen, Geburtsdatum, Geburtsort und Mitglieds-Nummern ihrer Mitglieder an ihren zuständigen Bundesverband zur Führung einer automatisierten Mitgliederdatei und zur Ausstellung von Spielerberechtigungsausweisen, Mannschaftslisten usw. zur Verfügung zu stellen. Mitglieder von Sportvereinen sowie von öffentlich-rechtlichen Berufsvertretungen beschwerten sich darüber, daß ihre Anschriften einer politischen Partei zur Wahlwerbung überlassen worden waren. Bestimmte Details der durch Computer ausgedruckten Adreßaufkleber ließen auf die Herkunft der Daten schließen.

In anderen Fällen war zu klären, ob ein Verein Anschriften seiner Mitglieder einer ihm angeschlossenen Einrichtung, etwa einem rechtlich selbständigen Zeitschriftenverlag, zwecks Direktwerbung überlassen darf.

Ich teile die Auffassung der Aufsichtsbehörden der Länder, daß die Zulässigkeit der Übermittlung in diesen Fällen vor allem an dem von der Vereinigung verfolgten Zweck, wie er sich z. B. aus der Satzung ergibt, zu messen ist. Die Mitgliedschaft ist als vertragsähnliches Vertrauensverhältnis im Sinne

des § 24 Abs. 1 erste Alternative BDSG anzusehen. Für die konkrete Ausgestaltung des Vereinszwecks sind insbesondere die ordnungsgemäß zustande gekommenen Beschlüsse des Vereins heranzuziehen. Nach diesen Grundsätzen gelangten die Aufsichtsbehörden, die über die konkreten Fälle zu entscheiden hatten, zu dem Ergebnis, daß die Weitergabe von Mitgliederdaten an Dachverbände oder an angeschlossene Organisationen auch unter dem Gesichtspunkt der Mitgliederbetreuung im allgemeinen als vom Vertragszweck gedeckt anzusehen ist. Sobald jedoch der Verwendungszweck beim Empfänger mit dem Vereinszweck nichts mehr unmittelbar zu tun hat, wie es etwa bei der Bereitstellung von Daten einer Berufs- oder Sportvereinigung für Zwecke der Wahlwerbung durch eine politische Partei der Fall ist, käme eine Übermittlung nur gemäß der zweiten Alternative des § 24 Abs. 1 Satz 1 BDSG in Betracht; dazu müßte in jedem Einzelfall festgestellt werden können, daß die berechtigten Interessen der Vereinigung oder des Empfängers den schutzwürdigen Belangen der Mitglieder vorgehen. Mit Recht hat die zuständige Aufsichtsbehörde in einem solchen Fall darauf hingewiesen, daß es entscheidend darauf ankommt, mit welcher Verwendung man als Vereinsmitglied rechnen muß, und daß der Betroffene im vorliegenden Fall nicht davon ausgehen konnte, daß der Verein seine Daten an eine politische Partei weitergibt.

Vielfach scheint den verantwortlichen Organen nicht bewußt zu sein, daß eine unbefugte Datenübermittlung auch strafrechtliche Konsequenzen nach sich ziehen kann (§ 41 BDSG). Mitunter wird aber wohl auch darauf vertraut, daß die Informationskanäle im dunkeln bleiben werden. In der Tat konnten die zuständigen Aufsichtsbehörden der Länder in mehreren Fällen nicht ermitteln, auf welchem Weg personenbezogene Daten von einer mutmaßlichen Herkunftsstelle zu einem bekannten Verwender der Daten gelangt waren. Hieraus ergibt sich die Notwendigkeit, kritisch zu beobachten, ob die Untersuchungsbefugnisse der Aufsichtsbehörden ausreichen.

4 Übergreifende Erfahrungen mit dem BDSG, Kritik, erste Änderungsvorschläge

Das BDSG ist schon während seiner Entstehung viel kritisiert worden; zu einem früheren Entwurf habe auch ich mich kritisch geäußert. Nachdem das Gesetz beschlossen und in Kraft getreten ist und seine Vorschriften durch praktische Maßnahmen verwirklicht werden müssen, hat es wenig Sinn, die bekannten Mängel nochmals aufzulisten, ohne die Praxis des Umgangs mit dem Gesetz zu berücksichtigen.

Jetzt kommt es darauf an, ob das Gesetz tatsächlich im Sinne eines möglichst wirksamen Schutzes von Bürgerrechten befolgt wird. Soweit aus heutiger Sicht Defizite festzustellen sind, müssen nicht nur Novellierungsvorschläge erarbeitet werden, sondern vorrangig sind alle Beteiligten aufgerufen, auf andere Weise als durch neue gesetzliche Vorschriften Abhilfe zu suchen. So steht es jedem Datenverarbeiter frei, von sich aus zusätzliche Maßnahmen des Datenschutzes zu ergreifen und von Vorbehaltsklauseln, die das Gesetz enthält, keinen Gebrauch zu machen. In diesem Sinne habe ich bereits mehrfach an die Bundesverwaltung appelliert (zum Beispiel in Fragen der Auskunftsverweigerung durch Sicherheitsbehörden). In diesen Zusammenhang gehört auch, daß manche speichernden Stellen auf die Erhebung eines Entgelts für die Auskunft an die Betroffenen verzichtet haben. Daß es umgekehrt auch Behörden und private Stellen gibt, die den Sinn des Gesetzes zu Gunsten einer „effektiveren" Verwaltung ihrer eigenen Angelegenheiten umkehren, ist bedauerlich.

Es wäre aber wirklichkeitsfremd anzunehmen, daß eine so neue und weitreichende Rechtsmaterie binnen kurzer Zeit vollständig und sinngerecht aufgenommen werden könne und daß vor allem ihre Notwendigkeit sogleich von der großen Mehrheit der Beteiligten rückhaltslos akzeptiert werde. Man muß auch bedenken, daß der Datenchutz mit anderen starken Interessen in Widerstreit gerät, vor allem mit dem im öffentlichen wie im privaten Bereich verbreiteten Interesse an möglichst vollständiger Absicherung der eigenen rechtlichen und wirtschaftlichen Position (das sich im privaten Bereich in Kreditschutzorganisationen, Auskunftsstellen der Versicherungswirtschaft u. ä., im öffentlichen Bereich in Informationssystemen der Sicherheitsbehörden und der Finanzverwaltung niederschlägt). Eine noch so intensiv betriebene Öffentlichkeitsarbeit stößt hier notwendigerweise an die Grenzen ihrer Wirksamkeit.

Für ein Urteil darüber, ob das BDSG sich praktisch bewährt habe oder nicht, ist es also noch zu früh. Mit diesem Vorbehalt ist das erste Jahr seiner Geltung indessen eher positiv zu bewerten. Eine wichtige Wirkung muß vorweg gewürdigt werden: Das Gesetz hat alle datenverarbeitenden Stellen genötigt, sich selbst und anderen Rechenschaft über die Art und Weise und die Notwendigkeit der Verarbeitung personenbezogener Daten in der jeweils gewählten Form zu geben. Wie erwartet, wurden die Generalklauseln des Gesetzes von den an extensiver Informationsverarbeitung interessierten Stellen jeweils in ihrem Sinne extensiv interpretiert, auch wenn die Datenschutzinstanzen dem entgegentraten. Oft begnügte man sich mit einer formalen Rechtfertigung wie der, daß bestimmte Angaben zu „Planungszwecken" oder zur „üblichen Betreuung" (eines Kunden) erforderlich seien. Wo eine solche Praxis über längere Zeit hin aufrecht erhalten wird, ist schließlich eine strengere Auslegung des BDSG undurchsetzbar; in solchen Fällen wird — wenn eine

weitere Erprobungszeit abgelaufen ist — ein bereichsspezifischer und damit konkreter Ansatz des Datenschutzes unvermeidbar sein. Soweit mein Kontrollbereich geht, werde ich jedoch zuvor versuchen, die zuständigen Stellen davon zu überzeugen, daß dem Sinn des BDSG nur eine restriktive Auslegung der „Aufgaben-/Erforderlichkeitsklausel" entspricht. International läßt sich eine gewisse Tendenz feststellen, die Registrierung von Datenbanken vorzuschreiben. Die deutschen Datenschutzgesetze schreiben eine Anmeldung nur für die öffentlichen Stellen und die „Fremdverarbeiter" im nicht-öffentlichen Bereich (§§ 31, 39 BDSG) vor. Ob der deutsche Gesetzgeber gut daran getan hätte, die Anmeldepflicht auf den gesamten Bereich privater Datenverarbeitung zu erstrecken, ist schwer zu beurteilen. Schweden, das sogar eine Lizenzierung aller „Personenregister" vorgeschrieben hat, macht damit, soweit ersichtlich, recht gute Erfahrungen; es ist nicht, wie man hätte befürchten können, eine große Datenschutzbürokratie entstanden, sondern eine relativ kleine Behörde, die den Arbeitsanfall bewältigt und nicht in Massenarbeit erstickt und die viel beachtete Zeichen auf dem Weg zu einem wirksamen Datenschutz gesetzt hat. Allerdings hat das Nachbarland Dänemark das Lizenzsystem in seinen vor kurzem erlassenen Datenschutzgesetzen nicht voll übernommen, sondern sich auf Registrierung beschränkt (vgl. unten 5.2.5).

Gelegentlich konnte beobachtet werden, daß nicht zu wenig, sondern zu viel — nämlich im falschen Zusammenhang — von Datenschutz gesprochen wurde: Es gab Versuche, das BDSG zu Zwecken zu mißbrauchen, für die es nicht erlassen wurde. So wurden einige berechtigte Auskunftswünsche, zum Beispiel zu Zwecken wissenschaftlicher Forschung, unter Hinweis auf ein angebliches Geheimhaltungsverbot nach dem Datenschutzrecht abgelehnt, zum Teil sogar bei reinen Sachdaten.

Es wird weiter zu beobachten sein, ob die Bestimmungen des BDSG in ihrer gegenwärtigen Fassung einer etwaigen Zweckentfremdung Vorschub leisten. Sollte sich das bei einer größeren Anzahl von Fällen bestätigen, würden Überlegungen zu einer entsprechenden Gesetzesänderung erforderlich. Gegenwärtig reichen die beobachteten Fälle hierfür jedoch noch nicht aus.

4.1 Anwendungsbereich des BDSG

4.1.1 Personenbezogene Daten

Die richtige Entscheidung des Gesetzgebers, alle personenbezogenen Daten in den Schutzbereich des Gesetzes einzubeziehen (weil auch „harmlose" Daten durch Umsetzung in einen anderen Zusammenhang „sensibel" werden können), ist in der Öffentlichkeit häufig falsch verstanden worden. So ist es vielfach zu einer rein quantitativen Betrachtungsweise gekommen: ein Vorhaben der Informationsverarbeitung wird allein deshalb für riskant erachtet, weil eine große Menge von Datenarten einbezogen werden soll. In vielen Fällen ist aber die Speicherung und Verarbeitung einer größeren Datenmenge tolerierbar. So erwachsen aus jeder rechtlichen Verbindung — aus einem geschäftlichen Kontakt wie dem des Käufers zu einem Verkäufer oder des Versicherungskunden zu einem Versicherungsunternehmen, aus einem Arbeitsverhältnis und aus einem öffentlich-rechtlichen Rechtsverhältnis wie dem des Sozialversicherten zu seiner Krankenkasse, Berufsgenossenschaft oder Rentenversicherungsanstalt — eine Reihe von Daten, die sich schnell zu einer Vielzahl summieren (Name, Vorname, eventuell Geburtsname, Geburtstag und Geburtsort — die zur eindeutigen Identifizierung des Betroffenen bei einem großen Teilnehmerkreis unverzichtbar sind —, Beruf, Datum der Aufnahme der Rechtsbeziehungen, Höhe des Entgelts oder Beitrags, eventuelle Zuschläge, geleistete Zahlungen, für die Überweisung von Geldbeträgen angegebene Konten und Bankinstitute usw.).

Eine kritische Betrachtung muß bei den einzelnen Daten und ihren möglichen Kombinationen ansetzen, sie muß also *qualitativer* Art sein. Bei komplexen Rechtsverhältnissen mit vielen Besonderheiten (unterschiedliche Ausgestaltung eines Versicherungsverhältnisses während verschiedener Fristen, Kinder- und Altenzuschläge beim Gehalt und bei der Steuer) können recht umfangreiche Datensammlungen unvermeidbar und auch unproblematisch sein, während ein knapp gehaltener Fragebogen, der Angaben zu bestimmten Lebensbereichen (Gesundheit, Verhaltensweisen, Anschauungen) aufnehmen soll, trotz seiner Kürze datenschutzrechtlich unzulässig sein kann. Schon das Bekanntwerden einer einzigen Art von Information, etwa einer Angabe über die Zugehörigkeit zu einer bestimmten Organisation, kann für den Betroffenen Nachteile mit sich bringen, die von Rechts wegen nicht entstehen sollen.

Die speichernden Stellen könnten viel dazu beitragen, den Bürgern eine genauere Vorstellung von der spezifischen Art ihrer jeweiligen Datenverarbeitung zu vermitteln. Leider haben sie diese Chance bisher nur in sehr geringem Maße wahrgenommen. So sind die Benachrichtigungen nach § 26 und § 34 BDSG regelmäßig so formuliert: „Wir informieren Sie, daß wir Daten über Sie gespeichert haben". Damit wird eher Beunruhigung hervorgerufen als die vom Gesetz erwartete Aufklärungsarbeit geleistet. Es ist zu hoffen, daß die künftige bereichsspezifische Gesetzgebung hier zu einem differenzierteren Sprachgebrauch nötigen wird.

4.1.2 Anknüpfungspunkt Datei

Die Vorschriften des BDSG wie auch der Landesdatenschutzgesetze greifen nur ein, wenn personenbezogene Daten in einer Datei verarbeitet oder aus einer Datei übermittelt werden. Die Datei ist also die „Relevanzschwelle": was unterhalb dieser Grenze mit den Angaben einer Person geschieht, wird von dem Datenschutzgesetz ignoriert. Die Frage, welche Datensammlungen Dateien im Sinne des BDSG sind, ist daher von zentraler Bedeutung für die Reichweite des Gesetzes. In der Fachliteratur hat sich noch keine einheitliche Linie herausgebildet. So

wird z. B. die Anzahl der Merkmale, nach denen eine Datensammlung sortierbar sein muß, um den Dateibegriff zu erfüllen, teils mit zwei, teils mit vier, von manchen aber auch mit drei angegeben. Gelegentlich wird auch die Ansicht vertreten, daß die Möglichkeit der Umsortierung nicht genüge, sondern daß entsprechende Verfahren auf die jeweilige Sammlung auch tatsächlich angewendet werden müßten, damit diese eine Datei im Sinne des BDSG sei. Man mag in dieser Auslegung lediglich einen erfolglosen Versuch sehen, den Anwendungsbereich des BDSG einzuschränken. Insgesamt bewirkt die Unterschiedlichkeit der Interpretationen aber doch eine gewisse Unsicherheit in Grenzfällen, die anläßlich einer späteren Novellierung durch eine entsprechende Neuformulierung beseitigt werden müßte.

So notwendig es unter den Gesichtspunkten der Praktikabilität und der Verhältnismäßigkeit war, einen Rahmen abzustecken, so wenig kann doch übersehen werden, daß die vom Gesetz gewählte Lösung den Betroffenen vielfach nicht einleuchtet.

So ist es beispielsweise einem Bürger, der sich um einen Kredit bemüht, kaum begreiflich zu machen, daß die Mitteilung seines Kreditgesuchs an eine Auskunftei (zur Einholung einer Auskunft) ein datenschutz-irrelevanter Vorgang sein soll (weil nämlich seine Angaben noch nicht aus der Akte in die Datei übernommen worden sind), während die Meldungen über den Abschluß und den weiteren Verlauf des Kreditvertrages nur im Rahmen des BDSG zulässig sind. Worauf es dem Betroffenen vor allem ankommt, ist die streng zweckgebundene Verwendung seiner Angaben. Er möchte es beispielsweise ausgeschlossen wissen, daß sein Arbeitgeber sich über Einzelheiten seiner privaten Sphäre unterrichten kann, etwa über aufgenommene Kredite oder über Auseinandersetzungen vor Behörden und Gerichten. Dieses Schutzbedürfnis besteht auch schon vor Aufnahme der betreffenden Daten in eine Datei. Soweit das BDSG nicht anwendbar ist, ist der Betroffene zwar keineswegs rechtlos: In einer Reihe von Fällen greifen spezialgesetzliche Schutzbestimmungen ein, und darüber hinaus sind die Grundsätze des allgemeinen Persönlichkeitsrechts, wie sie von der Rechtsprechung entwickelt wurden, nach wie vor anzuwenden.

Die verschiedenen Elemente dieses Rechtsschutzsystems sind jedoch nicht aufeinander abgestimmt, sondern haben unterschiedliche Ansätze und daher auch unterschiedliche Wirkungsweisen. Vor allem müssen die erwähnten allgemeinen Rechtsprinzipien aus der Rechtsprechung abgeleitet, können also nicht aus Gesetzestexten abgelesen werden — was ihre Zugänglichkeit für die Betroffenen erschwert.

Für den Betroffenen ist allein entscheidend, welche Stellen welche Angaben über ihn sammeln und unter welchen Bedingungen sie diese Angaben Dritten bekanntgeben. Auf welche technische und organisatorische Weise diese Vorgänge ablaufen, ist ihm gleichgültig; er kennt die Einzelheiten nicht und hat auf sie auch keinerlei Einfluß. Das BDSG nötigt jedoch, wie gesagt, zu Unterscheidungen nach der Art des gewählten Verfahrens. Das hat zum Beispiel zur Folge, daß manche speichernden Stellen, die mit sensiblen Daten arbeiten, versuchen, den Regelungen des BDSG durch restriktives Verständnis des Dateibegriffes zu entgehen. So stellte sich bei einem Besuch einer Krankenkasse heraus, daß der dortige Datenschutzbeauftragte die Ansicht vertrat, die Kartei der Leistungsdaten sei keine Datei im Sinne des BDSG, weil ein Umordnen nach anderen als den der vorhandenen Ordnung zugrunde liegenden Merkmalen zwar möglich, aber nicht sinnvoll sei. Abgesehen davon, daß es durchaus Verwaltungszwecke geben kann, die eine Umordnung als sinnvoll erscheinen lassen, stellt § 2 Abs. 3 Nr. 3 BDSG nur auf die Möglichkeit des Umordnens ab. Die zitierte Rechtsansicht ist also unhaltbar; ich bin ihr entgegengetreten und werde auch ähnliche Versuche, den Anwendungsbereich des BDSG zu verkleinern, abwehrenn.

Zur Klarstellung sei — aus Anlaß von Anfragen, die an mich gerichtet wurden — noch folgendes festgestellt:

Solange personenbezogene Angaben in einer Datei gespeichert sind, ist ihre Übermittlung durch das BDSG beschränkt, ohne daß es im Einzelfall darauf ankommt, ob sie aus der Datei selbst, einer entsprechenden Liste, den Eingabebelegen oder einer inhaltlich mit ihnen übereinstimmenden Akte entnommen werden. Es wäre eine Verkennung des Gesetzessinns, wollte man seine Anwendung schon dann aufhören lassen, wenn in Dateien gespeicherte Daten nur in eine andere Darstellungsform übersetzt würden. Die einfache Abschrift könnte dann schon den gesetzlichen Schutz beenden. Nur dort, wo unter den Voraussetzungen für die Anwendung einzelner Vorschriften bestimmte Erscheinungsformen der Daten oder bestimmte Verarbeitungsmethoden genannt sind, ist die Anwendung dieser Vorschriften an die jeweils genannten Voraussetzungen gebunden; dies gilt zum Beispiel für die Anlage zu § 6 Abs. 1 Satz 1.

4.1.3 Interne Dateien

Als problematische Einengung des Anwendungsbereichs des BDSG hat sich die Vorschrift des § 1 Abs. 2 Satz 2 erwiesen. Danach gilt für Daten, die in Handkarteien (also nicht automatisiert) geführt werden und lediglich internen Zwecken dienen (also nicht zur Übermittlung an Dritte bestimmt sind) von den Vorschriften des Gesetzes nur § 6. Es ist leicht einsichtig, daß in diesen Fällen z. B. die Festlegung von Zulässigkeitsvoraussetzungen für Datenübermittlungen entbehrlich ist. Zu fragen ist aber, weshalb der Gesetzgeber solchen Daten auch den Schutz des § 5 versagt hat, wonach die bei der Datenverarbeitung beschäftigten Personen die Daten nicht entgegen deren Zweckbestimmung nutzen dürfen und auf das Datengeheimnis zu verpflichten sind.

§ 5 ist die einzige Vorschrift des Gesetzes, die über die in § 1 Abs. 1 genannten Datenverarbeitungsarten hinaus allgemein die unbefugte sonstige Nutzung in die Verbotsregelung einbezieht. Sie unter-

sagt damit auch die unbefugte Weitergabe von Daten innerhalb einer Behörde oder eines Unternehmens und regelt damit einen Tatbestand, der gerade für interne Dateien durchaus relevant werden kann. Aber auch die unbefugte Übermittlung interner Daten an Dritte stellt sich möglicherweise in ihrer Wirkung als schwerwiegender dar als bei Daten, die schon nach ihrer allgemeinen Zweckbestimmung Dritten zugänglich gemacht werden dürfen.

Der Verzicht auf die Verpflichtung auf das Datengeheimnis sowie beispielsweise auch auf die strafrechtlichen Folgen mißbräuchlicher Datenverarbeitung (§ 41 BDSG) läßt sich jedenfalls nicht aus einem minderen Schutzbedürfnis der Betroffenen in diesen Fällen erklären. Die gleiche Problematik stellt sich möglicherweise auch hinsichtlich weiterer nicht anwendbarer Vorschriften des Gesetzes.

4.1.4 Medienprivileg

4.1.4.1 Gefahren für Persönlichkeitsrechte

Als eine Lücke im Datenschutz wird auch die Medienklausel von den Betroffenen empfunden — jene Bestimmung also, die Presse, Rundfunk und Film im Hinblick auf das Grundrecht nach Artikel 5 GG von der Beachtung der Vorschriften des BDSG freistellt (ausgenommen § 6; vgl. § 1 Abs. 3). So ist mir mehrfach die Frage vorgelegt worden, wie bestimmte Veröffentlichungen über persönliche Angelegenheiten mit dem Datenschutz zu vereinbaren seien. In einem Fall wurde etwa die Praxis einer Lokalzeitung bemängelt, regelmäßig die Gerichtstermine in Strafsachen in folgender Form anzukündigen: „Amtsgericht X. (Zimmer 21), 8.45 Uhr Bauarbeiter Günther F. (Y-Dorf) angeklagt wegen Trunkenheit am Steuer, ... 10.00 Uhr Waldarbeiter Helmut W. (Z-Dorf". Ich konnte mich davon überzeugen, daß es bereits mit Hilfe des Telefonbuches und eines veröffentlichten Adreßbuches möglich war, Betroffene eindeutig zu identifizieren. Ich lasse dahingestellt, ob die Publikation von Angaben, die aus einer öffentlichen Gerichtsverhandlung oder einer vor dem Gerichtssaal ausgehängten Prozeßliste stammen, mit dem Persönlichkeitsrecht, so wie es das Bundesverfassungsgericht insbesondere in der Lebach-Entscheidung (BVerfGE 35, 202) verdeutlicht hat, vereinbar ist. Es kommt in diesem Zusammenhang lediglich darauf an, besonders darauf hinzuweisen, daß die Grenzen der Anwendbarkeit des Bundesdatenschutzgesetzes keineswegs auch Grenzen für den Persönlichkeitsschutz des einzelnen darstellen. — In einem anderen Fall berichteten deutsche Presseorgane im Anschluß an die Explosionskatastrophe im Sommer 1978 auf einem spanischen Campingplatz über das Schicksal einzelner Betroffener deutscher Staatsangehörigkeit, wobei die Personalien (Namen, Anschriften, zum Teil auch Geburtsdaten und Paßnummer) und Einzelheiten der erlittenen — teilweise sehr schweren — Gesundheitsschäden mitgeteilt wurden.

Soweit mir bekannt geworden ist, stammten diese Angaben nicht von deutschen Behörden, sondern waren von den örtlichen spanischen Stellen durch private Agenturen und Vereinigungen (Automobilclub) vermittelt an deutsche Nachrichtenredaktionen gelangt. Auch unter Berücksichtigung der besonderen Umstände dieses Unglücksfalles halte ich es für bedenklich, wenn Gesundheitsdaten einzelner Bürger personenbezogen ohne deren Einwilligung veröffentlicht werden. Die Benachrichtigung von Angehörigen der von Unfällen Betroffenen ist zunächst Aufgabe der Behörden; wenn die Medien dabei in unkonventioneller Weise mitwirken, sollten sie dabei auch die Persönlichkeitsrechte der Verunglückten wahren. Es wäre zu begrüßen, wenn entsprechende Grundsätze durch Organe der Medien-Selbstkontrolle erarbeitet würden. Eine entsprechende Initiative eines Abgeordneten des Deutschen Bundestages ist leider bisher erfolglos geblieben.

4.1.4.2 Medienprivileg für öffentliche Stellen?

Im Kreise der Datenschutzreferenten des Bundes ist die Auffassung vertreten worden, bei Literatur-Dateien und Forschungsprojekt-Dateien, die der Herstellung *behördlicher Publikationen* dienen, könne das Presseprivileg zum Zuge kommen, vorausgesetzt, daß die publizistische Aktivität durch organisatorische Maßnahmen von dem übrigen Bereich der Behörde klar abgeschottet sei.

Ich kann mich dieser Auffassung nicht anschließen. Eine Behörde kann sich durch publizistische Aktivitäten nicht in ein Unternehmen der Presse verwandeln und sich insoweit von der Beachtung des Datenschutzes dispensieren. Das Medienprivileg ist geschaffen worden, um dem Grundrecht der Pressefreiheit bzw. der Freiheit der Berichterstattung (Artikel 5 Abs. 1 GG) auch in diesem Bereich Rechnung zu tragen (so auch Begründung zu § 2 des Regierungsentwurfs, BT-Drucksache 7/1027). An diesem Zusammenhang zwischen der Medienklausel und den Grundrechten nach Artikel 5 GG ist auch die Auslegung des § 1 Abs. 3 BDSG zu orientieren. Eine Anwendung auf Behörden und sonstige öffentliche Stellen ist danach grundsätzlich ausgeschlossen. Etwas anderes gilt nur, soweit öffentliche Stellen selbst Träger der Grundrechte nach Artikel 5 GG sind, wie etwa die öffentlich-rechtlichen Rundfunkanstalten.

Ich habe die obersten Bundesbehörden gebeten, bei den Meldungen zum Dateienregister und bei der Veröffentlichung nach § 12 BDSG entsprechend zu verfahren.

4.2 Zuordnung einiger Organisationen zu den verschiedenen Abschnitten des BDSG

4.2.1 Öffentlich-rechtliche Wettbewerbsunternehmen

Bei der Frage, ob eine datenverarbeitende Stelle dem öffentlichen oder dem nicht-öffentlichen Bereich zuzuordnen und demgemäß nach dem zweiten oder dem dritten Abschnitt des BDSG zu behandeln ist, sind bisher nennenswerte Schwierigkeiten nicht aufgetreten.

Eine öffentlich-rechtliche, der Aufsicht des Bundes unterstehende Versicherungsanstalt hat geltend gemacht, sie könne im Hinblick auf ihre Tätigkeit als Privatversicherungsunternehmen und ihre Teilnahme am Wettbewerb nicht als öffentliche Stelle im Sinne des § 7 Abs. 1 BDSG angesehen werden. Ich habe demgegenüber klargestellt, daß das Gesetz bei der Zuordnung zum öffentlichen Bereich — und damit zu meinem Kontrollbereich — ausschließlich von der Rechtsform ausgeht. Soweit es sich bei den öffentlichen Stellen allerdings um Unternehmen handelt, die am Wettbewerb teilnehmen, sieht das Gesetz weitgehend die Anwendung der gleichen Datenschutzvorschriften vor wie bei ihren privatrechtlich organisierten Konkurrenten. Dies ändert aber nichts daran, daß es sich um öffentliche und daher vom Bundesbeauftragten zu kontrollierede Stellen handelt. Die anfragende Versicherungsanstalt hat inzwischen ihre Dateien zu dem von mir geführten Dateienregister angemeldet.

4.2.2 Kontrollkompetenz bei bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts

Gemäß § 19 Abs. 1 BDSG kontrolliert der Bundesbeauftragte für den Datenschutz die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz bei den in § 7 Abs. 1 BDSG genannten Behörden und sonstigen Stellen des Bundes ... § 7 Abs. 1 BDSG bestimmt, daß die Vorschriften des zweiten Abschnittes des BDSG (§§ 7 bis 21) für Behörden und sonstige öffentliche Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gelten.

Aus dem unterschiedlichen Wortlaut der §§ 7 und 19 BDSG ist anfänglich von einer bundesunmittelbaren Körperschaft des öffentlichen Rechts gefolgert worden, sie falle nicht unter die Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz. Dieser Standpunkt wurde nach nochmaliger Überprüfung aber nicht aufrechterhalten.

Die Regelungen über den institutionellen Kontrollbereich finden sich in § 7 Abs. 1 und § 8 Abs. 3. Diese Vorschriften bestimmen den Kreis der Behörden und sonstigen (öffentlichen und nicht-öffentlichen) Stellen, auf welche die Vorschriften des zweiten Abschnitts des BDSG, also auch diejenigen über die Kontrolle durch den Bundesbeauftragten, Anwendung finden. Einer Wiederholung dieser in § 7 Abs. 1 und § 8 Abs. 3 getroffenen Regelungen bedurfte es daher in § 19 nicht. § 19 Abs. 1 hätte sich mit einer Verweisung auf § 7 Abs. 1 begnügen und dann zusätzlich die Personenvereinigungen des privaten Rechts (§ 8 Abs. 3) und die Gerichte (§ 19 Abs. 1 Satz 1 a. E.) regeln können.

Diesen Weg hat der Gesetzgeber nicht gewählt, sondern in § 19 Abs. 1 die Aufzählung des § 7 Abs. 1 nur teilweise wiedergegeben. Das ändert aber nichts an der Tatsache, daß er die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts der Kontrolle des Bundesbeauftragten unterworfen hat, zumal der in § 19 Abs. 1 verwandte Begriff „Behörden und sonstige öffentliche Stellen des Bundes" die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts umfaßt. Anderenfalls liefe das BDSG in einem wichtigen Bereich der automatischen Datenverarbeitung, dem der Sozialversicherung, praktisch weitgehend leer. Eine entsprechende gesetzgeberische Absicht kommt aber im BDSG nirgendwo zum Ausdruck. Die Prüfungskompetenz des BfD wird auch dadurch bestätigt, daß nach Feststellung von Verstößen gegen die Vorschriften des BDSG oder andere Datenschutzbestimmungen oder von sonstigen Mängeln bei der Verarbeitung personenbezogener Daten diesbezügliche *Beanstandungen* bei bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ auszusprechen sind (§ 20 Abs. 1 Nr. 3). Beanstandungen setzen eine Prüfung voraus. Wenn also gegenüber bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen Beanstandungen nach dem BDSG möglich sind, dann müssen vorher Prüfungen durchgeführt werden können.

4.2.3 Vereinigungen von Körperschaften etc.

Gemäß § 7 Abs. 1 BDSG gelten die Vorschriften des zweiten Abschnitts für *Vereinigungen* bundesunmittelbarer Körperschaften, Anstalten und Stiftungen. Die Formulierung gab zu der Frage Anlaß, ob darunter nur Vereinigungen zu verstehen sind, die *nur* bundesunmittelbare Körperschaften, Anstalten oder Stiftungen zu Mitgliedern haben, oder auch solche, die *neben* bundesunmittelbaren Körperschaften, Anstalten und Stiftungen *auch* landesunmittelbare Körperschaften, Anstalten und Stiftungen als Mitglieder haben. Die Frage hat insbesondere für die Dachorganisationen der Sozialversicherungsträger erhebliche praktische Bedeutung.

Der Bundesbeauftragte für den Datenschutz hat sich von Anfang an auf den Standpunkt gestellt, daß nur die zweite Alternative dem Sinne des BDSG gerecht werden und in der Praxis zu brauchbaren Ergebnissen führen kann. Die Dachorganisationen, mit denen hierzu ein Meinungsaustausch erfolgte — nämlich der Verband Deutscher Rentenversicherungsträger e. V., der Hauptverband der gewerblichen Berufsgenossenschaften e. V., der Verband der Angestellten-Krankenkassen e. V. und der Verband der Arbeiter-Ersatzkassen e. V. —, haben sich diesem Standpunkt angeschlossen.

Für die Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung in Essen, einer Vereinigung von bundesunmittelbaren Körperschaften des öffentlichen Rechts und von Dachorganisationen der Sozialversicherungsträger in privatrechtlicher Rechtsform, ist ebenfalls von der Geltung des zweiten Abschnitts des BDSG auszugehen.

4.2.4 Datenverarbeitung im Auftrag von Stellen des Bundes

Der Datenschutzbeauftragte einer privatrechtlich organisierten Großforschungseinrichtung, deren Gesellschaftsanteile überwiegend von der Bundesrepublik Deutschland gehalten werden, hat angefragt, in welcher Weise bei Forschungsprojekten die Datenschutzverantwortung zwischen der auftraggebenden Bundesbehörde und der Forschungseinrichtung nach dem BDSG verteilt sei. Ich habe darauf hingewiesen, daß es bei der Verarbeitung von Daten im Rahmen von Forschungsprojekten entscheidend darauf ankommt, wer die Berechtigung zur Verfügung über die Daten hat. Ist dies die Forschungseinrichtung, so scheidet eine Auftragsverarbeitung gemäß § 8 Abs. 3 BDSG aus. In diesem Fall ist zu berücksichtigen, daß derjenige, dem Forschungsergebnisse in personenbezogener Form mitgeteilt werden sollen, Dritter im Sinne von § 2 Abs. 3 Nr. 2 BDSG ist mit der Folge, daß die Vorschriften über die Zulässigkeit der Übermittlung zu beachten sind. Nach § 3 und den in § 36 BDSG enthaltenen Grundsätzen ist eine Übermittlung nur mit Einwilligung des Betroffenen zulässig. Liegt dagegen nach der Anlage des Projekts die Verfügung über die Daten bei dem Auftraggeber, so sind die Vorschriften über die Auftragsverarbeitung zu beachten. Ein solcher Fall wird etwa vorliegen, wenn der Forschungseinrichtung Daten für Zwecke des Programmtests oder zur statistischen Analyse übergeben werden oder wenn sie die Daten von vornherein im Namen ihres Auftraggebers übernommen hat. Eine Abgrenzung kann nur im Einzelfall erfolgen.

Für den in der Praxis der Forschungseinrichtung nicht seltenen Fall, daß einer Bundesbehörde Rechenkapazität zur Verfügung gestellt wird, vertrat der Datenschutzbeauftragte die Auffassung, daß eine Auftragsverarbeitung nach § 8 Abs. 3 BDSG nicht vorliege, weil der jeweilige Auftraggeber allein und ausschließlich entscheide, welche Daten wann und in welcher Weise verarbeitet werden. Ich habe demgegenüber klargestellt, daß bereits die Auslagerung einzelner Funktionen, z. B. des Maschinenbetriebes, für die Anwendbarkeit des § 8 Abs. 3 BDSG — und damit für meine Kontrollzuständigkeit — ausreicht. Nach ihrem Schutzzweck erfaßt die Vorschrift alle Fälle, in denen bei der Forschungseinrichtung beschäftigte Personen derart mit den Daten des Auftraggebers in Berührung kommen, daß sie sie zur Kenntnis nehmen oder auf ihren Inhalt einwirken können.

4.3 Sonderprobleme des Verhältnisses zu den Religionsgesellschaften

Die öffentlich-rechtlichen Religionsgesellschaften unterliegen im Hinblick auf die von ihnen betriebene Verarbeitung personenbezogener Daten weder meiner Kontrolle noch grundsätzlich der der Bundesländer. Offen und strittig ist noch, ob und inwieweit die kirchlichen Einrichtungen und Werke, die in der Rechtsform einer juristischen Person des Privatrechts organisiert sind, der staatlichen Datenschutzkontrolle unterliegen. Das BDSG knüpft allein an die Rechtsform an, was zur Folge hätte, daß die Mehrzahl dieser Einrichtungen der Kontrolle der Aufsichtsbehörden der Bundesländer unterläge. Bei rechtlich selbständigen Trägern kirchlicher publizistischer Tätigkeit, kirchlichen Krankenhäusern und Schulen halte ich dies auch für angezeigt. Dem steht die im kirchlichen Bereich vertretene Auffassung gegenüber, Einrichtungen, die „in einem bestimmten organisatorischen Zusammenhang mit der verfaßten Kirche stehen und kirchliche Aufgaben erfüllen" (Staatliche und kirchliche Zuständigkeiten im Datenschutzrecht, Rechtsgutachten im Auftrag des Datenschutzbeauftragten der EKD, von M. Stolleis, S. 27), unterlägen dem BDSG nicht. Diese Frage wird noch weiterer Klärung bedürfen. Entscheidend ist, daß es keine datenschutzfreien Bereiche geben darf.

Die Evangelische Kirche in Deutschland hat am 10. November 1978 das Kirchengesetz über den Datenschutz (Amtsblatt der EKD S. 2) verabschiedet, das inzwischen von fast allen Landeskirchen übernommen worden ist. Für die katholische Kirche hat der Verband der Diözesen Deutschlands Ende 1977 den Entwurf einer Anordnung über den kirchlichen Datenschutz verabschiedet, der in den einzelnen Diözesen in kirchliches Recht umgesetzt wird.

Mit den für Fragen des Datenschutzes zuständigen Vertretern der EKD und des Kommissariats der Deutschen Bischöfe ist ein Gedankenaustausch über gemeinsam interessierende Fragen des Datenschutzes aufgenommen worden, der sicher zu einer Harmonisierung der Datenschutzpraxis im staatlichen und im kirchlichen Bereich beitragen kann.

Ein schwieriges Problem ist die Frage, unter welchen Voraussetzungen personenbezogene Daten aus dem staatlichen Bereich an kirchliche Behörden übermittelt werden dürfen. Nach § 10 Abs. 2 BDSG und der entsprechenden Vorschrift in den Landesdatenschutzgesetzen muß sichergestellt sein, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden. Es reicht nicht aus, daß die Kirchen lediglich Datenschutzgesetze erlassen; es muß auch sichergestellt sein, daß ihr Vollzug gewährleistet ist. Eine Überprüfung im Einzelfall durch die jeweils übermittelnde Stelle wäre sicher unzweckmäßig; es wäre aber zu erwägen, daß die Prüfung generell durch die jeweils zuständige Aufsichtsbehörde durchgeführt wird. In Rheinland-Pfalz wird dieses Verfahren durch den Ausschuß für Datenschutz bereits mit Erfolg praktiziert. In Bayern werden die Staatsministerien des Innern und für Unterricht und Kultus gemeinsam auf Antrag feststellen, ob in der öffentlich-rechtlichen Religionsgesellschaft ausreichender Datenschutz sichergestellt ist. Hinsichtlich der aus dem staatlichen Bereich übermittelten Daten unterliegen die Religionsgesellschaften nach Artikel 25 Abs. 2 des Bayerischen Datenschutzgesetzes auch der Kontrolle des Landesbeauftragten für den Datenschutz. In meiner gutachtlichen Stellungnahme zum Melderecht habe ich die Auffassung vertreten, daß die Meldebehörden den Kirchen nur noch die Daten ihrer Mitglieder mitteilen dürften. Dem wurde von kirchlicher Seite entgegengehalten, die Kirchen benötigten zur Erfüllung ihres seelsorgerischen Auf-

trags auch die Daten von andersgläubigen Familienangehörigen und ungetauften Kindern. Ich meine jedoch, diese Daten sollten von den Mitgliedern der Religionsgesellschaft erfragt statt durch die Verwaltung übermittelt werden.

Ich habe mich ferner dafür ausgesprochen, bei Veröffentlichungen über kirchliche Amtshandlungen (wie Taufen, Konfirmation/Firmungen, Hochzeiten) dem Betroffenen ein Widerspruchsrecht einzuräumen. Die vereinzelt noch zu beobachtende Praxis, Kirchenaustritte im Gottesdienst bekanntzugeben, halte ich datenschutzrechtlich für nicht vertretbar.

4.4 Kontroll- und Abwehrrechte des Betroffenen

Auf einem Gebiet haben sich die Regelungen des BDSG als dringend ergänzungsbedürftig erwiesen, nämlich auf dem des Adressenhandels und der Direktwerbung.

Viele Bürger beklagen sich über eine wachsende Flut von Werbesendungen. Ganz abgesehen davon, daß sie die Zusendungen als Belästigung empfinden, sind sie durch die Vorstellung beunruhigt, daß ohne ihr Zutun in großem Umfang mit ihren Daten gehandelt wird.

Daß der Adressenhandel in der Bundesrepublik ein erhebliches Volumen hat und auch nach Inkrafttreten des BDSG offensichtlich weiter floriert, kann fast jedermann aus seiner persönlichen Erfahrung bestätigen. Ein Verband, in dem sich zwanzig Unternehmen der Adressenhandels- und Direktwerbebranche zusammengeschlossen haben, verweist in einer Broschüre auf das „Leistungsverzeichnis der Mitglieder", in dessen Abschnitt „Privatadressen (Verbraucheradressen)" sich u. a. folgende Positionen finden: „Alleinstehende Frauen, Jagdscheininhaber, leitende Personen, Schulkinder".

Soweit Adressenverlage Daten von öffentlichen Stellen beziehen, haben das BDSG und, soweit ich sehe, die Datenschutzgesetze der Länder eine Klärung gebracht. Daten können aus dem öffentlichen Bereich nur noch entweder aus allgemein zugänglichen Unterlagen (z. B. Fernsprechverzeichnis) entnommen oder mit Einwilligung der Betroffenen übermittelt werden. Dies ist jedenfalls die im Bereich des Bundes geübte Praxis (vgl. zum Kraftfahrtbundesamt oben 3.6.2.1, zur Bundespost oben 3.6.3).

Die wichtigere Datenquelle des Adressenhandels sind freilich die nicht-öffentlichen Stellen, die Daten über eigene Zwecke verarbeiten (z. B. Handels- und Dienstleistungsunternehmen, Vereinigungen). Diese gehen offensichtlich davon aus, daß die schutzwürdigen Belange der Betroffenen, an denen nach § 24 Abs. 1 und 2 BDSG die Zulässigkeit der Übermittlung zu messen ist, nicht beeinträchtigt werden. So sah sich beispielsweise ein Versandhaus durch das BDSG nicht gehindert, die Anschriften der Besteller von sog. ehehygienischen Artikeln an einen Adressenhändler zu verkaufen. Auch nach einer Beanstandung durch die Aufsichtsbehörde hat das betroffene Unternehmen diesen Gewerbezweig keineswegs eingestellt, sondern lediglich mit dem Adressenverlag vereinbart, daß die gelieferten Daten künftig in seinem Auftrag vermietet werden.

Selbst wenn die Aufsichtsbehörden erreichen, daß § 24 BDSG restriktiver angewendet wird, wird es dabei bleiben, daß den Adressenverlagen in erheblichem Umfang personenbezogene Daten überlassen werden, ohne daß die Betroffenen dabei mitwirken. Ihr Schutz hängt daher entscheidend davon ab, daß sie gegenüber den Adressenverlagen und deren Kunden, den werbenden Unternehmen, über ausreichende Kontroll- und Abwehrrechte verfügen.

Zwar hat die Werbewirtschaft bereits erkannt, daß Werbemaßnahmen bei Adressaten, die diese Form der Reklame ablehnen, keinen Erfolg versprechen. Sie unterhält deshalb eine Liste der Privatpersonen, die keine Werbung per Post wünschen, und sorgt dafür, daß die betreffenden Daten in den Beständen der angeschlossenen Adressenverlage gelöscht werden („Robinson-Liste", geführt vom ADV-Adressenverleger- und Direktwerbeunternehmen-Verband, Postfach 12 06, 6370 Oberursel). In entsprechender Weise verfahren die Deutsche Postreklame GmbH, Postfach 1 62 45, 6000 Frankfurt a. M., und das Kraftfahrtbundesamt, Postfach 7 83, 2390 Flensburg. Auf diese Möglichkeiten weise ich anfragende Bürger hin. Derartige freiwillige Datenschutzmaßnahmen der Wirtschaft sind sehr zu begrüßen. Sie geben dem Bürger jedoch keinen Rechtsanspruch und werden nicht in der gesamten Adressenhandelsbranche angewendet.

Die Kontroll- und Abwehrrechte, die das BDSG dem Betroffenen gibt, haben sich auf dem Gebiet des Adressenhandels und der Direktwerbung als unzureichend erwiesen. Der Betroffene kann sich zwar an das jeweils werbende Unternehmen wenden, diesem weitere Werbezusendungen untersagen (ein Recht, das die Rechtsprechung als Ausprägung des Persönlichkeitsrechts schon vor Inkrafttreten des BDSG anerkannt hat, vgl. BGH NJW 1973, 1119) und — nachdem damit der Zweck der Datenspeicherung entfallen ist — Löschung seiner Daten gemäß § 27 Abs. 3 Satz 2 BDSG verlangen. Damit allein ist ihm aber wenig gedient, solange seine Daten von dem Adressenverlag weiterhin gespeichert, verkauft und vermietet werden. Dies zu verhindern, gibt das BDSG keine Handhabe. Der Betroffene scheitert bereits bei dem Versuch herauszufinden, welche Adressenverlage Daten über ihn gespeichert haben. Eine Anfrage bei dem werbenden Unternehmen führt regelmäßig nicht weiter. Eine politische Vereinigung, die per Direktwerbung um Spenden anhält, bescheidet anfragende Bürger auf einem hektographierten Merkblatt „Ihre Frage ist nicht die einzige dieser Art . . . Falls Sie . . . noch nicht gespendet haben, so wurde ihre Adresse gemietet. Bei welchem Adressenhändler dies war, ist nicht feststellbar. Die Adressen wurden zurückgegeben, wir haben keine Kopien." Ein Dienstleistungsunternehmen erklärt den Fragestellern, für die Adressenauswahl sei allein die von ihnen beauftragte Werbeagentur verantwortlich, und bittet vorsorglich „höflichst, weitere Zusendungen unbeachtet zu lassen". In anderen Fällen wird dem Betroffenen lapidar erklärt, auf die

Mitteilung der Datenquelle habe er keinen Rechtsanspruch.

Normalerweise müssen nicht-öffentliche Stellen den Betroffenen von der Speicherung seiner Daten benachrichtigen (§ 26 Abs. 1 BDSG). Bei geschäftsmäßiger Datenverarbeitung für fremde Zwecke, zu der auch der Adressenhandel zählt, ist diese Pflicht allerdings eingeschränkt. Sie greift erst ein, wenn die Daten erstmals übermittelt werden (wozu der Versand an den Betroffenen nicht rechnet, § 2 Abs. 2 Nr. 2). Die listenmäßige Übermittlung von Grunddaten (Namen, Titel, akademischer Grad, Anschrift) zuzüglich der Angabe über die Zugehörigkeit zu einer Personengruppe (§ 32 Abs. 3) löst die Benachrichtigungspflicht aber nicht aus (§ 34 Abs. 1 Satz 2 BDSG). Sollte sich die Auffassung der Werbewirtschaft durchsetzen, daß die Adressenhändler aufgrund dieser Vorschrift von der Benachrichtigungspflicht befreit sind, müßte die gesetzliche Regelung unbedingt korrigiert werden. Einschränkungen bei den Kontrollbefugnissen des Betroffenen gegenüber den Adressenhändlern sind vor allem deshalb sehr bedenklich, weil die einwandfreie Verwendung der Adressen durch deren Kunden praktisch unkontrollierbar ist.

In diesem Sinne hat auch die schwedische Dateninspektion kürzlich angeordnet, daß Unternehmen, die eine nicht vom Betroffenen selbst erhaltene Anschrift verwenden, in der Werbesendung ihre Datenquelle bekanntgeben müssen.

Dringend verbesserungsbedürftig sind auch die Abwehrrechte des Betroffenen. Bei richtigen Daten kann er in der Regel erst nach fünf Jahren Löschung verlangen (§ 35 Abs. 3 BDSG). Der bereits erwähnte von den Gerichten anerkannte Anspruch auf Unterlassung von Werbezuschriften sollte in das BDSG aufgenommen und dahin erweitert werden, daß der Betroffene auch von Adressenhändlern jederzeit die Löschung seiner Angaben verlangen kann.

4.5 Weitere Fragen der Anwendung des BDSG

4.5.1 Aufklärungspflicht nach § 9 Abs. 2

Nach § 9 Abs. 2 BDSG haben öffentliche Stellen, wenn sie beim Betroffenen Daten erheben, ihn über die Rechtsgrundlage bzw. die Freiwilligkeit seiner Auskünfte aufzuklären. Die große Bedeutung dieser Vorschrift, die vom Bundestag in das Gesetz eingefügt wurde, hat sich schon im ersten Jahr der Geltung deutlich herausgestellt. Die Bestimmung wird in der Praxis aber noch nicht hinreichend beachtet. Beispiele wurden bereits in anderen Zusammenhängen (Antrag auf Fernmeldeanschluß, oben 3.6.3, und Kundenkarte des Frankfurter Verkehrsverbundes, oben 3.6.2.2) mitgeteilt. Ein anderes Beispiel sei hinzugefügt: Ein Bürger, der mit einer Bausparkasse in Verhandlungen wegen des Kaufs eines Eigenheims stand, erhielt von dieser einen „Fragebogen für Bauinteressenten für ein Baugrundstück im Baugebiet XY". Im Begleitschreiben hieß es dazu, es sei mit der Gemeinde vereinbart, daß bei einem Verkauf der Grundstücke in unbebautem Zustand die Genehmigung der Gemeinde einzuholen sei. Um dieses Mitspracherecht ausüben zu können, erbitte die Gemeinde von den Bewerbern die Abgabe jenes Fragbogens. Die Bausparkasse erklärte, sie hoffe ein Grundstücksangebot „nach Abstimmung mit der Gemeinde . . . in absehbarer Zeit unterbreiten zu können". In dem Fragebogen wurde nicht nur nach der Zusammensetzung des Haushalts des Baubewerbers gefragt, sondern auch nach den Jahreseinkünften des Haushaltungsvorstandes, der Ehefrau, der Kinder und der sonstigen Haushaltsangehörigen, darüber hinaus nach der Höhe des vorhandenen Barkapitals, nach Bausparverträgen sowie danach, ob der Interessent oder seine Ehefrau bereits Haus- oder Grundeigentümer seien („Wenn ja: Was und Wo"), schließlich ob man eine Mietwohnung habe, mit wieviel Quadratmetern und ob diese ausreiche. Die Bitte des Bürgers, der Bausparkasse wie auch der Gemeinde „die Anweisung zu erteilen, Fragen solcher Art zu unterlassen", konnte ich nicht erfüllen. Eine Entscheidung der zuständigen Instanzen des Landes, an die ich die Angelegenheit weitergereicht habe, ist noch nicht ergangen. Ich berichte den Fall hier, um zu zeigen, in welch schwierige Lage ein Bürger geraten kann, wenn ihm — noch dazu im Zusammenhang mit einer erstrebten Leistung — die Aufklärung darüber vorenthalten wird, welche Angaben eine öffentliche Stelle nach gesetzlichen Bestimmungen verlangen darf und welche nur freiwillig erbeten werden.

Die Aufklärungspflicht nach § 9 Abs. 2 BDSG beruht auf der Erfahrung, daß viele Bürger, die von einer amtlichen Stelle zur Erteilung von Auskünften aufgefordert werden, annehmen, hierzu verpflichtet zu sein oder bei Weigerung mit Nachteilen rechnen zu müssen. Von Freiwilligkeit kann dann nicht mehr die Rede sein. Dies führt zu der Überlegung, ob nicht für die öffentliche Verwaltung auf die Einwilligung als Ermächtigungsgrundlage der Datenverarbeitung ganz verzichtet werden sollte (wie auch in den Beratungen des BDSG schon vorgeschlagen wurde). Solange dies nicht gilt, ist es unbedingt erforderlich, daß die Behörden bei ihrer Informationserhebung den beteiligten Bürgern soviel Aufklärung wie möglich über Sinn und Zweck der Datenerhebung sowie über Art und Weise der vorgesehenen Datenverarbeitung geben. Das Fragebogenwesen muß deshalb in fast allen Bereichen von Grund auf neu durchdacht werden. Manche Verwaltungen versuchen, sich dieser Konsequenz dadurch zu entziehen, daß sie alte Formulare mit Stempelaufdrucken versehen, welche die gesetzlichen Anforderungen des § 9 Abs. 2 wiedergeben.

Mit diesem — formal in der Regel nicht zu beanstandenden — Verfahren nehmen sich die Verwaltungen die Chance, ihre Arbeitsweise auf eine neue, bürgerfreundliche Basis zu stellen.

Dem Sinn der Vorschrift widerspricht es auch, wenn bloß Hinweise auf gesetzliche Vorschriften — gar in der Form von Paragraphenketten mit unverständlichen Abkürzungen und Verweisungen — angebracht werden. Vielmehr sollte das Gemeinte in allgemein verständlicher Sprache und bezogen auf die jeweiligen konkreten Verwaltungsvorgänge ausge-

drückt werden, wobei verschiedene, sich gegenseitig ergänzende Formen der Unterrichtung in Betracht kommen (schriftlich und mündlich, ferner Merkblätter, die zumindest interessierten Bürgern angeboten werden sollten).

4.5.2 Auskunftspraxis

Die Auskunft nach § 13 BDSG über die eigenen personenbezogenen Daten ist bisher bei keiner öffentlichen Stelle des Bundes (und — soweit ersichtlich — bei keiner Landesbehörde) zu einem quantitativen Problem geworden. Es sind bei allen Stellen nur wenige Auskunftsersuchen eingegangen. Trotzdem sind einige Fehler bei den beantragten Auskünften unterlaufen. Über enttäuschende Erfahrungen, die ein Abgeordneter des Hessischen Landtages, eine Vereinigung von Datenschutz-Interessenten und einige Journalisten bei Anfrageaktionen gemacht haben, ist in der Presse berichtet worden. Auch in verschiedenen Eingaben an mich wurden ungenügende Auskünfte gerügt (vgl. oben 3.5.2).

Ein nicht ganz selten vorgekommener Fehler besteht darin, daß nicht die tatsächlich gespeicherten Daten in die Auskunft aufgenommen werden, sondern daß in einem besonderen Schreiben mitgeteilt wird, welche Arten von Daten die betreffende Stelle zu speichern pflege. Damit wird dem Betroffenen die Möglichkeit genommen, die Richtigkeit der gespeicherten Daten zu überprüfen. Zu betonen ist auch, daß etwa benutzte Abkürzungen und Schlüsselzahlen dem Betroffenen erläutert werden müssen; sonst liegt keine verständliche Auskunft vor.

Für manche Dienststellen — zum Beispiel große Kommunalverwaltungen, die über eine Fülle verschiedener Dateien verfügen — war es schwierig, allgemein formulierten Auskunftsersuchen („Auskunft über alle meine Daten") gerecht zu werden. Die Auskunft soll so erteilt werden, daß der Bürger eine wirkliche und für ihn verständliche Information erhält. Hierfür kann es sich empfehlen, daß die speichernde Stelle ihm zunächst — natürlich kostenlos — mitteilt, welche Datenarten in welchen Verwaltungsbereichen gespeichert werden, um ihm die Gelegenheit zu geben, seine Auskunftswünsche näher zu präzisieren (vgl. die Soll-Vorschrift in § 13 Abs. 1 Satz 2 BDSG). Damit läßt sich zumindest vermeiden, daß der Bürger voller Erwartung auf aussagekräftige Dateiauskünfte eine Gebühr zahlt und sodann eine Vielzahl „harmloser" Aufzeichnungen mitgeteilt erhält (in vielen Dateien steht nur die Anschrift und eventuell die Kontonummer des Betroffenen). Ist jedoch erkennbar, daß der Betroffene eine vollständige Auskunft über alle ihn betreffenden Datenspeicherungen einschließlich der unproblematischen wünscht, so muß dieses Begehren erfüllt werden.

Manche Bürger haben Anstoß daran genommen, daß vor Erteilung von Auskünften ein Identitätsnachweis von ihnen verlangt wurde. Dies scheint mir jedoch gerade im Interesse des Datenschutzes notwendig. Es muß verhindert werden, daß jemand sich Auskünfte über Dritte erschleicht. Für den Nachweis der Identität gibt es viele Methoden. Bei häufigen Namen kann die Angabe des Geburtsdatums und eventuell auch des Geburtsortes nötig sein.

Auch im nicht-öffentlichen Bereich sind einige Probleme aufgetaucht. In der Frage, ob die auskunftspflichtige Stelle Vorauszahlung des Entgelts verlangen kann, haben sich die Aufsichtsbehörden dahin verständigt, daß ein solches Verlangen durch die § 26 Abs. 3, § 34 Abs. 3 BDSG nicht gedeckt ist. Im Hinblick darauf, daß die vom Betroffenen zu tragenden Kosten sich bei einer Zug-um-Zug-Leistung um die Nachnahmegebühr erhöhen, soll es jedoch nicht beanstandet werden, wenn die auskunftspflichtige Stelle zunächst einmal die Auskunft gegen Vorkasse anbietet. Auf Verlangen muß jedoch ein anderer Leistungsmodus bereitstehen.

Viele Stellen, bei denen häufig Auskünfte verlangt werden, haben hierfür Formulare ausgearbeitet. Ein solches Vorgehen kann zweckmäßig sein, wenn es dazu beiträgt, den Anfragenden einwandfrei als den Betroffenen zu identifizieren. Unbefriedigend ist es jedoch, wenn dem Betroffenen durch Inhalt und Ausgestaltung des Formulars ein falscher Eindruck von seiner Rechtsstellung vermittelt wird. Deshalb haben verschiedene Aufsichtsbehörden das von einigen Auskunfteien verwendete Formular beanstandet, in dem ohne erläuternde Zusätze neben den Angaben zur eigenen Person auch Angaben über den Ehegatten erfragt wurden und die Unterschriften beider Ehegatten vorgesehen waren. Zwar bestehen keine Bedenken, wenn aus Kostengründen zwei Auskunftsverlangen miteinander verbunden werden; es muß dann aber klargestellt werden, daß der Betroffene zwischen Einzel- und Ehegattenauskunft frei wählen kann und daß nur in letzterem Fall die Angaben und die Unterschrift des Ehegatten erforderlich sind.

Vielfach kleiden auskunftspflichtige Stellen ihre Entgeltforderungen in Formulierungen, die die Rechtslage nicht korrekt wiedergeben. So wird etwa durch die Formulierung: „Die durch die Bearbeitung dieses Antrags gemäß § 34 Abs. 3 BDSG entstehenden direkt zurechenbaren Kosten betragen . . . DM" der Eindruck erweckt, der verlangte Betrag ergebe sich unmittelbar aus dem Gesetz. Fast alle Auskunfteien betrachten im übrigen die Auskunftserteilung als günstige Gelegenheit, von dem Betroffenen eine Überprüfung der Angaben auf Vollständigkeit und Richtigkeit sowie Korrektur- und Ergänzungsangaben zu erbitten.

Erhebliche Verärgerung bei vielen Bürgern hat die gesetzliche Ermächtigung verursacht, für die Erteilung von Auskünften an die Betroffenen eine Gebühr bzw. ein Entgelt zu verlangen. Daß nicht alle speichernden Stellen von diesem Recht Gebrauch machten, fällt wenig ins Gewicht angesichts der immer wiederholten Beobachtung, daß Bürger sich für den Fall vollständiger Auskunftseinholung hohe Kosten errechnen und daraufhin von solchen Anträgen absehen. Es stößt auch auf wenig Verständnis, daß für Auskünfte über eigene Daten im Bereich der Bundesverwaltung eine Gebühr erhoben wird, die höher ist als die Gebühr der Meldebehörden für Registerauskünfte über Dritte. Da sich die von den Gesetzesverfassern gehegte Befürchtung, es

werde zu einer nicht zu bewältigenden Flut von Auskunftsersuchen kommen, die die Verwaltung in ihrer Arbeitsfähigkeit beeinträchtigen werde, nicht bewahrheitet hat, sollte die Gebühren- bzw. Entgeltpflichtigkeit der Auskünfte bei der nächsten Gelegenheit abgeschafft werden. Ich halte es für angebracht, solche Kosten für kleine Zusatzleistungen an den Bürger als allgemeine Aufwendungen der speichernden Stelle anzusehen, die durch die Vorteile der modernen Datenverarbeitung bei weitem kompensiert werden.

Sollten wider Erwarten doch noch unzumutbar viele Auskunftsersuchen eingehen, so kann notfalls auf die Bestimmung zurückgegriffen werden, daß die Auskunft unterbleiben kann, soweit sie die rechtmäßige Erfüllung der Verwaltungsaufgaben gefährden würde (§ 13 Abs. 3 Nr. 1 BDSG).

4.5.3 Dateienregister

Das von mir nach § 19 Abs. 4 BDSG zu führende Register der von den Bundesbehörden automatisch betriebenen Dateien bezweckt, den Bürgern eine Übersicht über die Verarbeitung personenbezogener Daten in der Bundesverwaltung zur Verfügung zu stellen und meine Kontrollaufgaben wirksam zu unterstützen. Diese Ziele werden zum Teil nur unvollständig und mit großem Aufwand zu erreichen sein. Dies liegt zum einen daran, daß weder die Datenschutzregisterordnung selbst noch das ihr beigefügte Muster des Meldevordrucks die erforderliche Spezifizierung deutlich genug zeigen. Aus der Begründung zur Datenschutzregisterordnung ergibt sich jedoch, daß die einzelnen Datenarten genau zu beschreiben sind, z. B. durch die Feldbezeichnung. Viele Stellen praktizieren die Verordnung aber so, daß die Meldungen nicht erkennen lassen, welche Angaben über die Betroffenen tatsächlich geführt werden. So bezeichnen einige Stellen die Art der gespeicherten personenbezogenen Daten lediglich durch allgemeine Umschreibungen wie „personalbezogene Daten, die bei der Beschäftigung von Personal wichtig sind"; andere lassen es bei Eintragungen wie „Anschriften und verschiedene Sortiermerkmale" oder „Fragebogenaktion" bewenden. Hier sind viele Rückfragen und Beratungen erforderlich. Zum anderen fallen die Dateien, die nicht automatisiert geführt werden, also z. B. alle Handkarteien, zwar unter die Veröffentlichungspflicht nach § 12 Abs. 1 BDSG, sie sind aber nicht zum Register anzumelden.

Damit ist die Übersicht für den Bürger sehr erschwert. Einen vollständigen Überblick erhält er nur anhand der Veröffentlichungen im Bundesanzeiger. Auch ich bin, obwohl ich ein Dateienregister zu führen habe, auf die ergänzenden Veröffentlichungen angewiesen, wenn ich ein vollständiges Bild über die Datenverarbeitung in der Bundesverwaltung gewinnen oder Bürgern, die sich ratsuchend an mich wenden, Hinweise geben will, wo sie ihr Auskunftsrecht geltend machen können. Den anmeldenden Stellen wird durch die teilweisen Überschneidungen der Meldungen zum Register und zur Veröffentlichung Doppelarbeit zugemutet.

Die Aussagekraft der Veröffentlichungen im Bundesanzeiger wird aller Voraussicht nach wesentlich geringer sein als die des Dateienregisters. Nach den mit den Registeranmeldungen gemachten Erfahrungen ist zu befürchten, daß viele Veröffentlichungen Mängel aufweisen. Es gibt aber keine zentrale Stelle, die für die Prüfung der Veröffentlichungen auf Klarheit, Vollständigkeit und einheitliche Form verantwortlich wäre. Es empfiehlt sich daher, zu prüfen, ob es nicht zweckmäßig ist, die Zuständigkeiten für die Veröffentlichung und für die Registerführung zu vereinigen, zumal beide Maßnahmen denselben Zweck erfüllen sollen (so die Regelung in Frankreich, vgl. 5.2.2).

4.6 Datensicherung

Unabhängig davon, daß Datensicherung schon bisher nach allgemeinen Prinzipien (vgl. auch § 5 Abs. 1 BDSG) geboten war, tritt am 1. Januar 1979 § 6 BDSG mit der Anlage zu § 6 Abs. 1 Satz 1 in Kraft. Diese Bestimmung schreibt vor, daß personenbezogene Daten verarbeitende Personen oder Stellen die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung des BDSG zu gewährleisten. Die Anlage zu § 6 Abs. 1 Satz 1 enthält für die automatische Datenverarbeitung „zehn Gebote" der Datensicherung. Das spätere Inkrafttreten dieser Regelungen sollte es allen Beteiligten ermöglichen, sich rechtzeitig auf die am 1. Januar 1979 entstehende Rechtslage einzustellen und geeignete Vorkehrungen zu treffen.

Um den Anwendern in Verwaltung und Wirtschaft eine Hilfe bei der Umsetzung der Datensicherungsvorschriften in konkrete Maßnahmen zu geben, hat die sog. „Münchener Runde" — ein Arbeitskreis, in dem sich unter Federführung Bayerns Vertreter der obersten Aufsichtsbehörden der Länder, des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz sowie interessierter Kreise der Wirtschaft zusammengefunden haben — einen Entwurf für Vorläufige Verwaltungsvorschriften zu § 6 und dessen Anlage ausgearbeitet. Der Entwurf erläutert diese Regelungen, interpretiert die darin verwendeten Datenverarbeitungsbegriffe und gibt Beispiele für Maßnahmen, mit denen die einzelnen Datensicherungsanforderungen der Anlage zu § 6 erfüllt werden können.

Einige Länder haben den Entwurf bereits in Kraft gesetzt. Ich habe mich an den Vorarbeiten beteiligt, weil diese Richtlinien für *alle* datenverarbeitenden Stellen in der öffentlichen Verwaltung und der Wirtschaft gleichermaßen von Bedeutung sind. Datensicherung ist zu einem großen Teil realisierter Datenschutz. Nur eine möglichst einheitliche Handhabung von Datensicherungsverfahren kann dem Bürger die Gewißheit verschaffen, daß Datenschutz mehr ist als nur ein gesetzliches Postulat. Ich halte es daher für wünschenswert, daß auch der Bund entsprechende Vorschriften erläßt.

Dies bedeutet allerdings nicht, daß nicht schon in der Vergangenheit die Notwendigkeit wirksamer Datensicherungsmaßnahmen von den Anwendern in der Bundesverwaltung erkannt worden wäre. Meine Mitarbeiter haben bei ihren Besuchern einer Reihe von Rechenzentren festgestellt, daß die Entwicklungsarbeiten an Datensicherungskonzepten laufen, allerdings bisher unterschiedlich weit gediehen sind. Dieser Bericht geht darauf an den diesbezüglichen Stellen ein.

Mit dem 1. Januar 1979 bekommt die Aufgabe der Datensicherung einen noch höheren Stellenwert, als sie bisher hatte. Ich werde daher diesen Bereich im kommenden Berichtsjahr noch stärker beobachten und darauf im nächsten Jahresbericht zurückkommen.

5 Internationale Fragen des Datenschutzes

5.1 Bedeutung für den BfD

Stand und Entwicklung des Datenschutzrechts außerhalb der Bundesrepublik Deutschland sind für mich von mehr als akademischem Interesse. Ich benötige diese Informationen und die damit verbundenen Kontakte, um meine Aufgaben angemessen erfüllen zu können. Mein gesetzlicher Auftrag, die Bundesregierung und die sonstigen meiner Kontrolle unterliegenden öffentlichen Stellen in Fragen des Datenschutzes zu beraten, läßt sich nur durchführen, wenn ich dabei auch Erfahrungen mit berücksichtigen kann, die im Ausland bei der Vorbereitung und Verwirklichung des Datenschutzes gemacht worden sind.

5.1.1 Hilfe in Einzelfällen

Im Berichtsjahr sind mehrere Bürger mit der Bitte um Hilfe an mich herangetreten, weil sie aus einem Nachbarland, in dem es noch kein Datenschutzgesetz gibt, mit Werbesendungen überschüttet wurden und überdies Grund zu der Annahme hatten, daß ihre Anschrift dort an Dritte weiter veräußert wurde.

Ich habe hier zunächst keine Möglichkeit der Hilfe gesehen und die Einsender darauf hingewiesen, daß Vorbereitungen für ein internationales Datenschutzübereinkommen aufgenommen worden seien. Später ergab sich aufgrund inzwischen aufgenommener Kontakte die Möglichkeit, eine Behörde in dem betreffenden Staat einzuschalten, die im Rahmen der ihr zu Gebote stehenden Möglichkeiten versuchen wird, die Löschung der Daten zu erreichen.

In einem anderen Fall wandte sich ein in Spanien lebender Deutscher an mich, dem die Ausweisung drohte, weil er vor etwa zehn Jahren in der Bundesrepublik wegen eines Rauschgiftdelikts verurteilt worden war. Er nahm an, die spanische Polizei sei auf einen Hinweis deutscher Polizeidienststellen an diese Information gelangt. Dies war nach meinen Feststellungen nicht der Fall. Ungeachtet dessen hat das Bundeskriminalamt den spanischen Polizeibehörden mitgeteilt, daß die Vorstrafe inzwischen in Bundeszentralregister gelöscht sei und der Betroffene nach deutschem Recht als unbestraft gelte. Ich rechne damit, daß derartige Hilfsersuchen künftig in verstärktem Maße an mich herangetragen werden.

5.1.2 Kontakte und Informationen

Zur Erfüllung dieser sich aus meinem gesetzlichen Auftrag ergebenden Aufgaben habe ich im Verlaufe des Berichtsjahres zahlreiche Kontakte mit Persönlichkeiten und Dienststellen im Ausland, die mit Fragen des Datenschutzes befaßt sind, aufgenommen. Den Schwerpunkt bildete ein Besuch bei der schwedischen Datenschutzkontrollbehörde, der Dateninspektion. Diese seit 1974 bestehende Einrichtung verfügt über einen reichen Erfahrungsschatz, der mir bereitwillig zur Verfügung gestellt wurde. Die Dateninspektion hat es erreicht, mit einem relativ begrenzten Mitarbeiterstab erhebliche Wirkungen zu erzielen und dem betroffenen Bürger auf unbürokratische und effektive Weise zu helfen.

Es bot sich ferner die Gelegenheit zu einem Gedankenaustausch mit dem künftigen Leiter der dänischen Datenschutzkontrollbehörde und dem dänischen Ombudsmann. Außerdem konnte ich mich während einer Konferenz der Ditchley Foundation in Ditchley bei Oxford über den Stand der Datenschutz-Diskussion in Großbritannien informieren.

Alle diese Gespräche bilden eine gute Basis für die vereinbarte künftige Zusammenarbeit. Derartigen Initiativen sind indessen aus zeitlichen und finanziellen Gründen Grenzen gesetzt. Ich nutze daher die Möglichkeit, an Besprechungen, die im Rahmen der OECD, des Europarats und der Europäischen Gemeinschaft zu Fragen des Datenschutzes durchgeführt werden, als Beobachter teilzunehmen. Hier bietet sich die Gelegenheit, mit einem Minimum an Aufwand ein Maximum an Informationen über den aktuellen Stand des Datenschutzrechts zu gewinnen. Gleichzeitig kann ich über erste praktische Erfahrungen bei der Durchführung der Kontrolle nach dem Bundesdatenschutzgesetz berichten.

5.2 Stand der Datenschutzgesetzgebung im Ausland

5.2.1 Allgemeines

Die Datenschutzgesetzgebung im westlichen Ausland beginnt sich zu entwickeln. Nach Schweden und der Bundesrepublik Deutschland haben seit 1977 Kanada, Frankreich, Dänemark, Norwegen, Neusee-

land und Österreich Datenschutzgesetze erlassen. Das allen Gesetzen gemeinsame Ziel, der Schutz der Persönlichkeitssphäre des Bürgers, wird auf sehr unterschiedliche Weise angestrebt. Dem Ansatz des BDSG am nächsten kommt das am 18. Oktober 1978 verabschiedete österreichische Datenschutzgesetz.

Die übrigen Staaten verzichten ganz oder teilweise auf generelle materielle Vorschriften, die die Zulässigkeit der Verarbeitung personenbezogener Daten regeln. Im Mittelpunkt dieser Gesetze stehen Datenschutzkontrollinstanzen, die mit unterschiedlichen Befugnissen bei der Errichtung von Informationssystemen mitzuwirken haben — von der bloßen Anhörung (Dänemark) bis zur Genehmigungspflicht (Schweden, Frankreich). Ich gebe nachstehend einen Überblick über den wesentlichen Inhalt der in den vergangenen zwei Jahren verabschiedeten Datenschutzgesetze:

5.2.2 Das französische Datenschutzgesetz

Das französische Datenschutzgesetz (Nummer 78 — 17) vom 6. Januar 1978 ist nach dem schwedischen und dem Datenschutzgesetz der Bundesrepublik Deutschland das dritte nationale Datenschutzgesetz innerhalb Europas. Es gilt grundsätzlich für die automatisierte Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich. Abweichend vom Regierungsentwurf schützt das Gesetz nicht die Daten über juristische Personen. Den Kern der gesetzlichen Regelungen bildet eine unabhängige staatliche Kontrollkommission, der es obliegt, die automatisierte Verarbeitung personenbezogener Daten zu überwachen. Staatliche Stellen, die personenbezogene Daten automatisiert verarbeiten wollen, benötigen eine vorherige Genehmigung, sofern es für die Datenverarbeitung keine ausdrückliche Rechtsgrundlage gibt. Unternehmen der Wirtschaft und andere Stellen im nicht-öffentlichen Bereich melden der Kommission die von ihnen beabsichtigte automatisierte Verarbeitung personenbezogener Daten an. Die Anmeldung muß bestimmte Angaben über die beabsichtigte Art der Datenverarbeitung enthalten, u. a.: Art der zu verarbeitenden Daten, ihre Quellen, Dauer der Speicherung und Empfänger der Daten, Verknüpfungen mit anderen Daten sowie Datensicherungsmaßnahmen. Sollen die Daten ins Ausland übermittelt oder im Ausland verarbeitet werden, ist auch dies anzugeben.

Die Kommission registriert diese Angaben und veröffentlicht alljährlich eine Liste, in der für jede genehmigte oder angemeldete Form der Datenverarbeitung folgende Angaben enthalten sind: Rechtsgrundlage, Bezeichnung der Verarbeitung und ihre Zweckbestimmung, die Stelle, der gegenüber der Betroffene seinen Auskunftsanspruch geltend machen kann sowie die Art der gespeicherten Daten und im Falle ihrer Übermittlung die Empfänger. Darüber hinaus kann sie im Einzelfall Überprüfungen an Ort und Stelle durchführen und die dazu erforderlichen Auskünfte und Unterlagen verlangen. Ferner beobachtet sie die Entwicklung der Datenverarbeitung im öffentlichen und privaten Bereich.

Jedermann hat grundsätzlich das Recht, es abzulehnen, daß ihn betreffende personenbezogene Daten automatisiert verarbeitet werden. Dieses Recht kann er wahrnehmen, weil er bei der Erhebung der Daten darüber zu unterrichten ist, ob er zur Beantwortung der Frage verpflichtet ist oder nicht, welche Folgen die Verweigerung der Antwort hat und für wen die Daten bestimmt sind. Weiter ist anzugeben, ob es einen Auskunfts- oder Berichtigungsanspruch gibt. Werden die Daten schriftlich, z. B. mittels Fragebogen erhoben, müssen die Angaben ebenfalls schriftlich fixiert sein. Ausnahmen von dieser Regelung sind nur für den Fall der Strafverfolgung zugelassen.

Personenbezogene Daten über Straftaten, Verurteilungen oder Sicherungsmaßnahmen dürfen nur von wenigen eigens bestimmten öffentlichen Stellen gespeichert und verarbeitet werden. Daten, die Aufschlüsse über die rassische Herkunft, politische, weltanschauliche oder religiöse Einstellungen oder die Zugehörigkeit zu einer Gewerkschaft geben, dürfen nur mit ausdrücklichem Einverständnis des Betroffenen gespeichert werden. Nur Kirchen, Weltanschauungsgemeinschaften und Gewerkschaften dürfen über ihre Mitglieder automatisiert betriebene Dateien führen. Sonstige Ausnahmen darf nur der Staatsrat im öffentlichen Interesse zulassen. Grundsätzlich ist es öffentlichen und privaten Stellen verboten, Entscheidungen über das Verhalten einer natürlichen Person allein auf automatisiert verarbeitete Unterlagen zu stützen.

Jedermann hat das Recht, gegen Zahlung einer Gebühr Auskunft über die über ihn gespeicherten Daten zu verlangen. Auskunft über medizinische Daten erfolgt über einen vom Betroffenen benannten Arzt. Ungenaue, mißverständliche oder überholte Daten sind von Amts wegen oder auf Antrag des Betroffenen zu berichtigen. In Streitfällen über die Richtigkeit der Daten liegt die Beweislast bei der speichernden Stelle, es sei denn, daß die Daten vom Betroffenen selbst stammen oder mit seinem Einverständnis gespeichert wurden.

Unzulässigerweise gespeicherte Daten sind zu löschen. Waren die berichtigten oder gelöschten Daten zuvor einem Dritten übermittelt worden, ist er zu benachrichtigen, sofern die Kommission keine Ausnahme zuläßt. Für den grenzüberschreitenden Transport personenbezogener Daten enthält das Gesetz noch keine eigenen Regelungen. Die Kontrollkommission kann aber vorschlagen, daß er von einer vorherigen Genehmigung abhängig gemacht oder durch Regierungserlaß bestimmten Beschränkungen unterworfen wird.

Die strafrechtlichen Sanktionen für die Verletzungen der Vorschriften des Gesetzes sind sehr einschneidend. Mit Gefängnis zwischen sechs Monaten und drei Jahren und Geldstrafe kann bestraft werden, wer personenbezogene Daten automatisiert verarbeitet, ohne die Kommission beteiligt zu haben. Die Verletzung materieller Vorschriften kann ebenfalls mit Gefängnis von ein bis fünf Jahren und Geldstrafe bis zu 2 Millionen Francs bestraft werden. Strafbar ist auch die Übermittlung besonders sensibler

Daten ohne die Einwilligung des Betroffenen und die zweckentfremdete Verarbeitung.

5.2.3 Das österreichische Datenschutzgesetz

Der österreichische Nationalrat hat am 18. November 1978 das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz, im folgenden: ÖDSG) verabschiedet.

Es entspricht der Grundkonzeption des Bundesdatenschutzgesetzes insofern, als es in stärkerem Maße als andere Datenschutzgesetze materielle Regelungen zum Umgang mit personenbezogenen Daten enthält. Darüber hinaus nimmt es aber auch Teile anderer gesetzgeberischer Konzeptionen auf, die sich bisher bewährt haben. Geschützt sind nicht nur die Daten natürlicher, sondern auch die juristischer Personen.

5.2.3.1 Verfassungsrechtliche Grundlegung

Der österreichische Gesetzgeber hat für den Datenschutz klare Rechtsgrundlagen geschaffen, indem er ein Grundrecht auf Datenschutz schuf und gleichzeitig die Gesetzgebungszuständigkeit für Fragen des Datenschutzes durch eine Verfassungsbestimmung dem Bund zuwies.

Das Grundrecht auf Datenschutz gibt jedermann einen Anspruch auf Geheimhaltung ihn betreffender personenbezogener Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens hat. Einschränkungen dieses Grundrechts sind nur unter bestimmten Voraussetzungen zulässig. Jedermann hat ein Recht auf Auskunft, wer Daten über ihn ermittelt oder verarbeitet, woher die Daten stammen, welcher Art und welchen Inhalts sie sind und wozu sie verwendet werden. Ferner gewährt die Verfassungsbestimmung einen Berichtigungsanspruch (Text bei 6.1).

5.2.3.2 Anwendungsbereich

Das Gesetz gilt über die vier im BDSG aufgeführten Phasen des Speicherns, Veränderns, Übermittelns und Löschens hinaus auch für das Ermitteln von Daten ohne Rücksicht auf die dabei angewendeten Verfahren. Es stellt nicht auf das Vorhandensein von Dateien ab, sondern gilt für das Verarbeiten von Daten im oder für den automationsunterstützten Datenverkehr — was sich im Verhältnis zum BDSG als Einengung darstellt. Das Gesetz gilt einheitlich für die Verarbeitung personenbezogener Daten im Bund, den Ländern und im privaten Bereich.

5.2.3.3 Kontrollorgane

Ebenso wie alle anderen bisher erlassenen Datenschutzgesetze sieht auch das ÖDSG ein System externer Kontrolle vor. Als Kontrollorgane werden eine Datenschutz-Kommission und ein Datenschutz-Rat eingerichtet. Ein weiteres wichtiges Kontrollmedium ist das Datenverarbeitungsregister. Dem Betroffenen, der sich durch die Verarbeitung sich auf ihn beziehender Daten in seinen Rechten beeinträchtigt fühlt, steht der Weg zu den Gerichten offen.

— Datenschutz-Kommission

Die Datenschutz-Kommission ist eine weisungsfreie Kollegialbehörde. Sie besteht aus vier Mitgliedern. Ihr Personal wird vom Bundeskanzleramt zur Verfügung gestellt, dem auch die sonstige Geschäftsführung obliegt. Die Aufgaben der Kommission sind im Gesetz festgelegt. Ihr obliegt u. a. die Überprüfung von Einzelfällen, die aufgrund von Beschwerden Betroffener an sie herangetragen werden. Sie kann auch aus eigener Initiative Untersuchungen, die sie für geboten hält, durchführen. Sie erteilt ferner die notwendigen Bewilligungen im internationalen Datenverkehr. Alle zwei Jahre legt sie dem Bundeskanzler einen Tätigkeitsbericht vor, der ihn mit einer Stellungnahme dem Nationalrat zuleitet. Soweit die Datenschutzkommission in Einzelfällen Entscheidungen trifft, haben diese den Charakter von Gerichtsentscheidungen. Die betroffenen Verwaltungsbehörden sind verpflichtet, mit den ihnen zu Gebote stehenden Mitteln unverzüglich den der Rechtsanschauung der Datenschutz-Kommission entsprechenden Zustand herzustellen. Als Rechtsbehelf gegen Entscheidungen der Kommission ist die Beschwerde beim Verwaltungsgerichtshof gegeben. Die Kommission kann auch Empfehlungen aussprechen, die an die jeweils zuständige oberste Verwaltungsbehörde zu richten sind. Der Empfehlung ist entweder binnen einer bestimmten Frist zu entsprechen oder es ist schriftlich zu begründen, warum dies nicht geschieht.

— Datenschutz-Rat

Der Datenschutz-Rat besteht aus Vertretern der im Nationalrat vertretenen Parteien, der Arbeitnehmer- und Arbeitgeberschaft, des Bundes, der Bundesländer, Städte und Gemeinden. Seine Aufgaben sind im Gesetz festgelegt. Er wirkt mit bei aufgrund des Gesetzes zu treffenden rechtspolitischen Entscheidungen; er beobachtet die Auswirkungen des Gesetzes und unterbreitet Vorschläge für dessen Ergänzung oder Änderung.

Die Datenschutz-Kommission und der Datenschutz-Rat sind bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist Einsicht in Akten, Datenträger und sonstige Einrichtungen der Verarbeitung von Daten zu gewähren und Auskunft zu erteilen.

5.2.3.4 Datenverarbeitungsregister

Beim Österreichischen Statistischen Zentralamt wird ein Datenverarbeitungsregister eingerichtet, das von jedermann eingesehen werden kann. Jede öffentliche und jede private Stelle, die der Registrierungspflicht unterliegt, erhält eine Registernummer. Diese Nummer hat den Zweck, bei jedem automationsunterstützten Datum im Falle seiner Übermittlung den Absender feststellen zu können. Der Betroffene kann durch Angabe der Registernummer die jeweils übermittelnde Stelle erfahren und sodann seine Rechte wahrnehmen. Da immer die Nummer der letztübermittelnden Stelle anzugeben ist, läßt sich der Weg eines Datums auch über mehrere Zwischenstationen zurückverfolgen.

5.2.3.5 Datenschutz im öffentlichen Bereich

— Zulässigkeitsvoraussetzungen

Innerhalb des öffentlichen Bereichs dürfen personenbezogene Daten für Zwecke des automationsunterstützten Datenverkehrs nur ermittelt und verarbeitet werden, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht oder soweit dies für die Erfüllung der der speichernden Stelle gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet. Die Zulässigkeit der Übermittlung ist an ähnlich strenge Voraussetzungen gebunden.

Sollen personenbezogene Daten in automationsunterstützten Systemen verarbeitet werden, sind dem Datenverarbeitungsregister die Rechtsgrundlage, der Zweck der Ermittlung, Verarbeitung und Übermittlung, die Art der Daten und der Kreis der Betroffenen anzugeben.

— Datenschutz-Verordnungen

Um einen weitgehend bereichsspezifischen Datenschutz zu gewährleisten, sind die obersten Behörden des Bundes und der Länder verpflichtet, für jede ihrer Aufsicht unterstehende öffentliche Stelle eine Datenschutzverordnung zu erlassen, in der je nach der Art der zu verarbeitenden Daten die Grundsätze für deren Ermittlung, Verarbeitung, Benutzung und Übermittlung festgelegt werden. Jede datenverarbeitende öffentliche Stelle hat darüber hinaus eine Betriebsordnung zu erlassen, in der die Einzelheiten der Verarbeitung und des Schutzes der Daten festgelegt werden.

— Rechte des Betroffenen

Dem Betroffenen ist nicht nur Auskunft über die über ihn gespeicherten Daten in allgemein verständlicher Form zu geben, ihm sind auch die Herkunft und die Rechtsgrundlagen binnen vier Wochen schriftlich mitzuteilen. Die Verweigerung der Auskunft ist ebenfalls schriftlich zu begründen. Für die Erteilung der Auskunft kann eine angemessene Gebühr erhoben werden.

Unrichtige Daten sind zu berichtigen oder zu löschen. Bestreitet der Betroffene die Richtigkeit eines Datums, obliegt es der speichernden Stelle, sie zu beweisen; es sei denn, daß die Daten ausschließlich auf Angaben des Betroffenen beruhen.

Jeder Betroffene kann sich beschwerdeführend an die Datenschutz-Kommission oder auch an eine andere sachlich zuständige Behörde wenden, wenn er meint, durch die Verarbeitung ihn betreffender Daten in seinen Rechten verletzt worden zu sein.

5.2.3.6 Datenschutz im privaten Bereich

— Zulässigkeitsvoraussetzungen

Im privaten Bereich dürfen personenbezogene Daten nur ermittelt und verarbeitet werden, soweit sich dies in Art und Umfang auf den berechtigten Zweck des Rechtsträgers beschränkt und dadurch schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Die Übermittlung an Dritte ist außerdem nur insoweit zulässig, als

— der Betroffene ausdrücklich schriftlich zugestimmt hat oder

— die Übermittlung einem berechtigten Zweck des Rechtsträgers dient oder

— zur Wahrung überwiegender berechtigter Interessen eines Dritten notwendig ist oder

— die Daten anonymisiert worden sind.

— Benachrichtigungs- und Registrierungspflichten

Das österreichische Datenschutzgesetz unterscheidet ebenso wie das BDSG zwischen der Verarbeitung für eigene Zwecke und anderen Verarbeitungen, ohne jedoch ins einzelne gehende materielle Regelungen zu treffen. Werden personenbezogene Daten für eigene Zwecke, d. h. über Personen verarbeitet, mit denen die speichernde Stelle in einem Vertragsverhältnis steht oder stand und die in der Regel nicht an Dritte übermittelt werden sollen, ist der Betroffene darüber bei Aufnahme der Verarbeitung seiner Daten zu informieren. Das Gesetz legt im einzelnen fest, was ihm dabei mitgeteilt werden muß.

Sollen personenbezogene Daten außerhalb von Vertragsverhältnissen automationsunterstützt verarbeitet werden, muß vorab die Registrierung dieser Verarbeitung beim Datenverarbeitungsregister beantragt werden. Dabei sind über die Art der beabsichtigten Verarbeitung bestimmte Angaben zu machen. Bestehen Bedenken gegen die Rechtmäßigkeit der Registrierung, entscheidet die Datenschutzkommission.

— Rechte des Betroffenen

Die Rechte des Betroffenen entsprechen im wesentlichen denen im öffentlichen Bereich. Einen ausdrücklichen Schadensersatzanspruch gibt das Gesetz nicht, wohl aber einen Unterlassungs- und Beseitigungsanspruch. Rechtsstreitigkeiten sind vor den ordentlichen Gerichten auszutragen. Die Datenschutz-Kommission kann einem Verfahren als Nebenintervenient beitreten. Auf Ersuchen des Gerichts kann sie Gutachten über technische und organisatorische Fragen des Datenschutzes abgeben.

5.2.3.7 Internationaler Datenverkehr

Die Übermittlung personenbezogener Daten durch öffentliche und private Stellen ins Ausland bedarf grundsätzlich der Genehmigung der Datenschutz-Kommission. Nur in bestimmten im Gesetz aufgeführten Fällen kann darauf verzichtet werden. Das Gesetz legt ferner fest, unter welchen Voraussetzungen die Genehmigung zu erteilen ist. Sollen Daten ausländischer Rechtsträger in Österreich verarbeitet werden, ist dies dem Datenverarbeitungsregister zu melden. Soweit völkerrechtliche Vereinbarungen es vorsehen, kann auch eine Genehmigungspflicht vorgeschrieben werden.

5.2.3.8 Straf- und Schlußbestimmungen

Die widerrechtliche Offenbarung oder Verwertung sowie die Löschung, Verfälschung und sonstige Veränderung von personenbezogenen Daten in der Absicht, dem Betroffenen einen Schaden zuzufügen, kann mit Freiheitsstrafe bis zu einem Jahr bestraft werden. Die Verletzung von Informations- und Registrierungspflichten kann als Ordnungswidrigkeit mit Geldstrafe bis zu 150 000 Schilling geahndet werden.

Das Gesetz tritt am 1. Januar 1980 in Kraft. Die Mitglieder der Datenschutz-Kommission und des Datenschutz-Rats sind bis zum 1. April 1979 zu bestellen.

5.2.4 Datenschutz in Schweden

Schweden ist das erste Land, das den Datenschutz im öffentlichen und im privaten Bereich geregelt hat. Das schwedische Datenschutzgesetz vom 11. Mai 1973 gilt für automatisiert geführte Personenregister. Diese bedürfen einer Genehmigung der Datenschutz-Kontrollbehörde (Datainspektionen). Für den besonders sensiblen Bereich des Kreditauskunfteiwesens ist am 1. Juli 1974 das Kreditauskunftsgesetz erlassen worden (Deutsche Übersetzungen beider Gesetze in: Dammann/ Mallmann/Simitis, Die Gesetzgebung zum Datenschutz, Band 5 der Reihe Kybernetik, Datenverarbeitung, Recht; Veröffentlichungen der Forschungsstelle für juristische Dokumentation, Frankfurt 1977, S. 129 ff.).

Beide Gesetze haben sich in den ersten Jahren ihres Bestehens im wesentlichen bewährt. Eine zur Überprüfung des Datenschutzgesetzes gebildete Kommission hat im Herbst 1978 ihren Bericht vorgelegt und nur relativ geringfügige Änderungen vorgeschlagen. Einige davon könnten auch für die Diskussion in der Bundesrepublik Deutschland von Interesse sein:

— Das System der Genehmigung von Personenregistern soll beibehalten bleiben. Bei der Bearbeitung von Anträgen sollen Art und Umfang der zu speichernden Daten sowie die Zweckbestimmung des Registers besonders sorgfältig geprüft werden.

— Schon jetzt werden etwa 65 % aller Anträge nach einem vereinfachten Verfahren bearbeitet, da es sich um Register handelt, von denen offensichtlich keine Gefährdungen der Persönlichkeitssphäre zu befürchten sind. Die Kommission regt an zu prüfen, ob für derartige Register lediglich eine Anmeldung ausreiche.

— Register, die für Zwecke der Forschung und Statistik angelegt worden sind, sollen durch Datenschutzerwägungen in ihrer Funktionsfähigkeit nicht unnötig beeinträchtigt werden.

— Bei der Direktwerbung unter Verwendung von Anschriften aus öffentlichen Registern soll stets sorgfältig geprüft werden, in welcher Form die Daten genutzt werden dürfen.

Die Erteilung von Auskünften nach § 10 des schwedischen Datenschutzgesetzes ist in Einzelfällen auf erhebliche Schwierigkeiten gestoßen, wenn die Auskunft aus Registern erteilt werden mußte, die nur vorübergehend zu Testzwecken, für Forschungsvorhaben, zur Erstellung von Statistiken oder zur Erfüllung anderer Hilfsfunktionen bestanden. Die uneingeschränkte Auskunftspflicht bringt bei diesen Dateien erhebliche Schwierigkeiten mit sich, ohne jedoch dem Betroffenen wesentliche Informationen zu erbringen. Die Kommission spricht sich daher in derartigen Fällen für gewisse Ausnahmemöglichkeiten aus.

Eine beachtenswerte Besonderheit gilt nach einer Entscheidung der Dateninspektion vom Juni 1978 für die Anschriftenübermittlung zu Werbezwecken: In der Werbesendung muß angegeben werden, woher die Anschriften bezogen wurden. Würde dieses Gebot übernommen, so könnten wahrscheinlich manche Besorgnisse, die in bezug auf den privaten Adressenhandel wie auf die behördliche Datenübermittlung bestehen, ausgeräumt werden.

5.2.5 Datenschutzgesetze in Dänemark

Dänemark hat — ebenso wie Schweden und Norwegen — den Weg der bereichsspezifischen Gesetzgebung zur Regelung des Datenschutzes gewählt. Am 8. Juni 1978 wurden

— das Gesetz über öffentliche Register, 1978 (Gesetz Nr. 294) und

— das Gesetz über private Register, 1978 (Gesetz Nr. 293) erlassen. Beide Gesetze treten am 1. Januar 1979 in Kraft.

5.2.5.1 Das Gesetz über öffentliche Register

Das Gesetz über öffentliche Register (im folgenden als Datenschutzgesetz bezeichnet) gilt für in der öffentlichen Verwaltung geführte automatisiert betriebene Register, in denen personenbezogene Daten gespeichert sind. Ausgenommen sind Register der Polizei und der Nachrichtendienste. In Einzelfällen kann das Gesetz auf manuel geführte Register angewendet werden.

Eine Datenschutzbehörde überwacht die Einhaltung des Gesetzes.

Für jedes Register, das im Anwendungsbereich des Gesetzes eingerichtet werden soll, sind Richtlinien zu erlassen, in denen die allgemeinen Datenschutzvorschriften des Gesetzes, bezogen auf die im Register gespeicherten Daten konkretisiert werden. Vor dem Erlaß jeder Richtlinie ist die Datenschutzbehörde anzuhören.

Jede Richtlinie hat sich an folgenden generellen Regelungen zu orientieren:

Zulässigkeit der Speicherung

— Es dürfen nur Daten gespeichert werden, die für die Erfüllung der Aufgaben der Behörde erforderlich sind. Werden in einem Register Daten anderer Behörden im Auftrag gespeichert, ist sicherzustellen, daß nur die auftraggebende Behörde Zugriff zu diesen Daten hat.

— Besonders sensible Daten (z. B. Daten über rassische Zugehörigkeit, religiöse Überzeugungen, Vorstrafen, Gesundheit) dürfen grundsätzlich nicht gespeichert werden, es sei denn, daß sie für die Erfüllung des Zweckes des Registers erforderlich sind.

— Überholte Daten sind zu löschen. Durch Prüfverfahren soll sichergestellt werden, daß keine unrichtigen oder mißverständlichen Daten gespeichert werden.

— Für eine angemessene Datensicherung ist Sorge zu tragen.

Zulässigkeit der Übermittlung an Private

An private Unternehmen dürfen personenbezogene Daten aus behördlichen Registern nur weitergegeben werden, wenn der Empfänger sie benötigt, um für die öffentliche Stelle eine Aufgabe zu erfüllen. Sie dürfen zu keinem anderen Zweck verwandt werden. In allen anderen Fällen ist die Zustimmung des Betroffenen herbeizuführen, wobei dieser über die Art der zu übermittelnden Daten, den Empfänger und die beabsichtigte Verwendung zu unterrichten ist. Für medizinische Daten gelten besondere Regelungen.

An andere öffentliche Stellen können personenbezogene Daten insoweit weitergegeben werden, als diese sie zur Erfüllung ihrer gesetzlich festgelegten Aufgaben benötigen, oder wenn sie sie zur Herbeiführung einer Entscheidung unbedingt benötigen.

Rechte des Betroffenen

— Jedermann ist auf Antrag über die über ihn gespeicherten Daten zu unterrichten. Für einzelne Register kann die jeweils zu erlassende Richtlinie vorsehen, daß dem Betroffenen in bestimmten Abständen Auszüge aus dem Register vorzulegen sind.

— Auskünfte über in Registern gespeicherte medizinische Daten sind über den behandelnden Arzt zu erteilen.

— Eine Auskunft ist nicht zu erteilen, wenn überwiegende öffentliche oder private Interessen entgegenstehen, desgleichen nicht, wenn es sich um Register handelt, die ausschließlich für statistische Zwecke geführt werden.

— Die Auskunft wird einmal jährlich kostenfrei gegeben.

Datenschutzbehörde

Die Datenschutzbehörde besteht aus einem Rat und dem Sekretariat. Der Rat setzt sich aus dem Vorsitzenden und sechs weiteren Mitgliedern zusammen. Er wird auf jeweils vier Jahre bestellt.

Die laufenden Geschäfte erledigt das Sekretariat. Die Datenschutzbehörde kontrolliert die Einhaltung der Vorschriften des Gesetzes. Sie hat Zugang zu allen vom Gesetz erfaßten Registern. Sie kann Vorschläge zur Verbesserung des Datenschutzes, namentlich zur Ergänzung einzelner Richtlinien machen und die für ein Register verantwortliche Behörde auf Mängel hinweisen. Alljährlich ist dem Parlament ein Tätigkeitsbericht zu erstatten. Die Behörde kann überdies ihre Stellungnahmen und Einzelvoten veröffentlichen.

Die Verletzung der Vorschriften des Gesetzes kann mit Geldstrafe oder Gefängnis geahndet werden.

5.2.5.2 Das Gesetz über private Register

Neben dem Datenschutzgesetz, das für automatisierte Register in staatlichen Behörden gilt, hat das dänische Parlament am 8. Juni 1978 auch das Gesetz über private Register erlassen.

Das Gesetz gilt für die Verarbeitung personenbezogener Daten in automatisierten Registern, die normalerweise der Öffentlichkeit nicht zugänglich sind. Es gilt nicht für Register, die ausschließlich wissenschaftlichen oder statistischen Zwecken, der genealogischen Forschung oder als Hilfsmittel für Veröffentlichungen dienen.

Das Gesetz regelt den Datenschutz in bestimmten Branchen, in denen besonders vielfältige oder besonders sensible Daten verarbeitet werden. Dies sind die Bereiche Handel und Gewerbe, Auskunfteien, Adressenhandel und Service-Rechenzentren.

Handel und Gewerbe

Personenbezogene Daten dürfen in diesem Bereich nur insoweit verarbeitet werden, als dies zur Erfüllung der normalen Geschäftszwecke erforderlich ist. Daten über Rasse, Hautfarbe, religiöse oder politische Überzeugungen, Gesundheit oder Drogenmißbrauch dürfen nur mit Zustimmung des Betroffenen gespeichert werden, wobei diesem bewußt sein muß, daß die Daten in dem Register gespeichert werden sollen.

Warnregister über sogenannte „faule Kunden" dürfen nur mit Genehmigung der Datenschutzbehörde eingerichtet werden. In der Lizenz kann festgelegt werden, daß bestimmte Datenarten nicht in das Register aufgenommen werden dürfen. Die in § 3 Abs. 1 aufgeführten besonders sensiblen Daten dürfen nur mit Zustimmung des Betroffenen, andere Daten nur dann an Dritte übermittelt werden, wenn dies zur Erfüllung der Geschäftszwecke erforderlich ist. Nach Ablauf von fünf Jahren dürfen auch sie nur noch mit Zustimmung des Betroffenen übermittelt werden. Der Betroffene kann verlangen, daß unrichtige oder mißverständliche Daten berichtigt und unzulässigerweise gespeicherte Daten gelöscht werden. Lehnt die speichernde Stelle ein derartiges Verlangen ab, kann sich der Betroffene an die Datenschutzkontrollbehörde wenden, die eine abschließende Entscheidung trifft. Entscheidet sie zugunsten des Betroffenen, hat die speichernde Stelle alle bisherigen Empfänger über die vollzogene Berichtigung oder Löschung zu unterrichten. Alle automatisiert gespeicherten Daten sind kontinuierlich daraufhin zu überprüfen, ob sie noch zur Erfüllung des ursprünglichen Zweckes relevant sind. Ist das nicht der Fall, sind sie zu löschen.

Auskunfteien

Unternehmen, die personenbezogene Daten zum Zwecke der Ermittlung der finanziellen Verhältnisse und der Kreditwürdigkeit speichern, um sie an Dritte weiterzugeben, dürfen entsprechende Register nur nach vorheriger Registrierung durch die Datenschutzbehörde errichten. Gespeichert werden dürfen nur Daten, die zur Erfüllung des Zweckes der Register erforderlich sind. Daten über relevante Tatbestände, die mehr als fünf Jahre zurückliegen, dürfen nicht mehr registriert oder weitergegeben werden, es sei denn, daß sie von überragender Bedeutung für die Entscheidung über die Kreditwürdigkeit des Betroffenen sind.

Die o. g. besonders sensiblen Daten dürfen weder gespeichert noch weitergegeben werden. Name, Anschrift und Beruf sowie Daten, die behördlichen Amtsblättern oder öffentlich zugänglichen Amtsblättern entnommen sind, können frei gespeichert werden. Werden darüber hinaus andere Daten gespeichert, ist der Betroffene binnen vier Wochen darüber zu unterrichten und darauf hinzuweisen, daß er von seinem Auskunftsrecht Gebrauch machen kann. Von dieser Verpflichtung kann der Justizminister nach Anhörung der Datenschutzbehörde Ausnahmen zulassen. Der Auskunftsanspruch umfaßt alle gespeicherten Daten, nicht jedoch die Quellen, aus denen die Informationen stammen. Schriftliche Auskünfte werden gegen ein Entgelt erteilt, dessen Höhe der Justizminister bestimmt. Falsche oder mißverständliche Daten sind zu löschen oder zu berichtigen. In Streitfällen entscheidet die Datenschutzbehörde, die auch für die Kontrolle des Datenschutzes im öffentlichen Bereich nach Maßgabe des dänischen Datenschutzgesetzes zuständig ist.

Adressenhandel

Unternehmen, die Anschriften über Personengruppen sammeln und veräußern oder im Auftrag anderer Stellen selbst direkt werben, dürfen nur Namen, Anschriften, Berufe sowie offene Daten, die Handelsregistern entnommen sind, und schließlich Angaben über Interessen oder andere Merkmale speichern, die geeignet sind, die Personen bestimmten Gruppen zuzuordnen. Informationen über Rasse, sexuelle Besonderheiten, Hautfarbe, politische, religiöse Anschauungen, Vorstrafen, Gesundheit und Drogenmißbrauch dürfen nicht gespeichert werden. Der Justizminister kann weitere Einschränkungen anordnen. Jedermann kann verlangen, daß alle ihn betreffenden Daten gelöscht werden. Namenslisten, die den Unternehmen zum Zwecke der direkten Übersendung von Werbematerial zugeleitet worden sind, dürfen nur mit Zustimmung des Auftraggebers an Dritte weitergegeben werden.

Service-Rechenzentren

Rechenzentren, die personenbezogene Daten für Dritte im Auftrag verarbeiten, sind bei der Datenschutzbehörde zu registrieren. Sie dürfen die ihnen überlassenen Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

Datenverarbeitung außerhalb Dänemarks

Personenbezogene Daten, die in Dänemark nicht gespeichert und verarbeitet werden dürfen, dürfen auch nicht außerhalb des Landes erhoben und gespeichert werden. Sollen andere Daten außerhalb Dänemarks gespeichert werden, bedarf es einer Genehmigung durch die Datenschutzbehörde, sofern die Datenspeicherung in Dänemark selbst registrierungspflichtig wäre. Die Übermittlung personenbezogener Daten ins Ausland zum Zwecke der Verarbeitung ist nur mit Genehmigung der Datenschutzbehörde zulässig. Die Genehmigung wird nur dann erteilt, wenn die Daten auch im Empfängerland ausreichenden Datenschutz erfahren.

Kontrolle des Datenschutzes

Die Datenschutzbehörde überwacht die Einhaltung der Vorschriften des Gesetzes und der zu seiner Durchführung erlassenen Rechtsvorschriften. Sie kann sowohl aus eigener Initiative als auch auf Beschwerden Betroffener hin tätig werden. Sie hat das Recht, alle für die Kontrolle relevanten Informationen zu verlangen. Personenbezogene Daten, die nach Auffassung der Datenschutzbehörde nicht hätten gespeichert werden dürfen oder die falsch bzw. mißverständlich sind, sind auf Anordnung der Datenschutzbehörde zu löschen oder zu berichtigen. Sie kann auch bestimmte Verfahren zur Sammlung und Übermittlung von personenbezogenen Daten wegen der damit verbundenen Gefahren verbieten oder sie unter Auflagen zulassen. Die Datenschutzbehörde pflegt auch die Zusammenarbeit mit anderen Datenschutzkontrollbehörden im Ausland.

Verletzungen der Bestimmungen dieses Gesetzes können mit Geldstrafe oder mit Gefängnis bestraft werden.

5.2.6 Das norwegische Datenschutzgesetz

Das norwegische Datenschutzgesetz vom 9. Juni 1978 enthält die grundlegenden Vorschriften zum Schutz personenbezogener Daten in staatlichen, kommunalen sowie in bestimmten privaten Registern.

Die Kontrolle des Datenschutzes obliegt einem Datenüberwachungsdienst, der dem vom König benannten Fachminister untersteht. Der Überwachungsdienst berät die Regierung in den Fällen, in denen diese Entscheidungen nach dem Datenschutzgesetz zu treffen hat. Darüber hinaus beobachtet er die Entwicklung im Hinblick auf die Nutzung von Informationssystemen, die personenbezogene Daten enthalten, berät in Fragen des Datenschutzes und überwacht die Einhaltung der gesetzlichen Bestimmungen. Er führt ein Register aller Informationssysteme, die einer staatlichen Genehmigung bedürfen. Das Register ist jedermann zugänglich. Dem Datenüberwachungsdienst sind zur Erfüllung seiner Aufgaben alle Informationen verfügbar zu machen. Ausnahmen kann nur der König aus Gründen staatlicher Sicherheit anordnen.

Für alle Informationssysteme im öffentlichen und privaten Bereich gilt:

— Personenbezogene Daten dürfen nur gespeichert werden, wenn sie nach objektiven Kriterien zur Erfüllung des jeweiligen Zwecks erforderlich sind.

— Besonders sensible Daten, nämlich solche

  — über rassische Zugehörigkeit, politische oder religiöse Anschauungen,

  — Vorstrafen,

  — Gesundheit, Drogenmißbrauch,

  — Sexualleben,

  — familiäre Verhältnisse

  dürfen grundsätzlich nicht gespeichert werden.

— Jedermann hat einen Auskunftsanspruch über die über ihn in automatisierten Informationssystemen gespeicherten Daten. Ausgenommen sind Register, die statistischen oder planerischen Zwekken dienen. Dem Betroffenen kann die Auskunft ferner verweigert werden, wenn sie sich nachteilig auf seine Gesundheit oder die Beziehungen zu ihm nahestehenden Personen auswirken würde.

— Jedermann hat das Recht, die Berichtigung falscher, die Ergänzung unvollständiger und die Löschung obsoleter Daten zu verlangen.

— Jedes automatisiert geführte Register, das der Verarbeitung personenbezogener Daten dient, bedarf der staatlichen Genehmigung, desgleichen alle sonstigen Register, in denen die oben erwähnten besonders sensiblen Daten gespeichert werden sollen. Zusammen mit der Genehmigung wird im einzelnen folgendes bestimmt:

  — welche Arten von Daten gespeichert und wie sie verarbeitet werden,

  — an wen die Daten übermittelt werden,

  — ob das Personenkennzeichen verwendet werden darf,

  — welche Daten dem Auskunftsrecht des Betroffenen unterliegen,

— Verfahren zur Berichtigung, Ergänzung und Löschung von Daten,

— welche Datensicherungsmaßnahmen getroffen werden müssen.

Neben diesen generellen Vorschriften für Informationssysteme aller Art enthält das Gesetz Regelungen über den Datenschutz in bestimmten Branchen der Wirtschaft, nämlich für Kreditauskunfteien, Adressverlage, Service-Rechenzentren, Markt- und Meinungsforschungsunternehmen. Alle diese Unternehmen bedürfen vor Aufnahme ihrer Tätigkeit der staatlichen Genehmigung, die unter Auflagen erteilt und mit Bedingungen verbunden werden kann.

5.2.7 Stand der Datenschutzdiskussion in anderen europäischen Ländern

In den westeuropäischen Staaten, die noch keine eigene nationale Datenschutzgesetzgebung haben, sind die Vorbereitungsarbeiten dafür inzwischen aufgenommen worden und unterschiedlich weit gediehen.

5.2.7.1 Belgien

Aus Belgien ist im Jahre 1976 ein Gesetzentwurf bekannt geworden, der neben Regelungen über die automatisierte Verarbeitung von Daten über natürliche und juristische Personen auch Bestimmungen über das heimliche oder gegen den Willen des Betroffenen erfolgende Aufnehmen von Gesprächen oder das Fotografieren von Personen enthielt. Letzteres soll unter Strafe gestellt werden. Die Vorschriften über den Datenschutz bei der automatisierten Datenverarbeitung sind — mit einigen Abweichungen — denen des französischen Datenschutzgesetzes vergleichbar. Dieser Entwurf wird z. Z. von der belgischen Regierung überarbeitet. Im Dezember 1978 haben Neuwahlen stattgefunden. Wann nunmehr die Regierung einen neuen Entwurf vorlegt, ist noch offen. Dem Vernehmen nach wird auch erwogen, eine den Datenschutz betreffende Regelung in die Verfassung aufzunehmen.

Ein Entwurf eines Meldegesetzes, durch das ein Personenkennzeichen eingeführt werden soll, liegt ebenfalls vor. Er wird voraussichtlich um einige Datenschutzbestimmungen angereichert werden.

5.2.7.2 Luxemburg

Dem luxemburgischen Parlament liegt ein Gesetzentwurf vor, der sich auf die automatisierte Datenverarbeitung in öffentlichen und privaten Datenbanken bezieht. Er enthält materielle Regelungen über die Zulässigkeit der Sammlung und Speicherung von personenbezogenen Daten: Daten über politische und weltanschauliche Ansichten, die Gewerkschaftszugehörigkeit und über Einzelheiten des Privatlebens dürfen nicht erhoben und in Datenbanken gespeichert werden. Für Daten aus dem Bereich der Verbrechensbekämpfung und des Jugendschutzes wird ein staatliches Erhebungs- und Speicherungsmonopol begründet.

Der Betroffene ist bei der Erhebung der Daten über die beabsichtigte Verwendung, die Rechtsgrundlage oder die Freiwilligkeit und ggf. die Empfänger zu unterrichten.

Datenbanken, die im privaten Bereich errichtet werden, bedürfen der vorherigen Genehmigung durch den Minister, der für die Führung des nationalen Datenbankregisters zuständig ist. Bei der Entscheidung wird er durch einen aus fünf Mitgliedern bestehenden Beratungsausschuß unterstützt. Beabsichtigt die Regierung eine Datenbank zu errichten, soll sie nach dem Entwurf verpflichtet sein, den Ausschuß davon zu unterrichten, wobei sie die gesetzliche Grundlage bezeichnen soll.

Alle genehmigten oder angemeldeten Datenbanken werden in einem nationalen Datenbankregister geführt. Der für das Register zuständige Minister nimmt gleichzeitig Kontrollfunktionen im Hinblick auf die Datenbanken wahr. Jedermann kann das Register einsehen und von dem Betreiber einer Datenbank Auskunft über die über ihn gespeicher-

ten Daten verlangen. Sind sie unrichtig, unvollständig oder unzulässigerweise gespeichert, kann er die Berichtigung, Ergänzung oder Löschung verlangen.

5.2.7.3 Niederlande

In den Niederlanden wird ebenfalls ein Gesetz vorbereitet, mit dessen Verabschiedung im Verlaufe des Jahres 1980 gerechnet wird. Die Errichtung, Verwaltung und Anwendung von automatisierten Informationssystemen in der Zentralverwaltung vollzieht sich gegenwärtig nach Richtlinien der niederländischen Regierung vom 7. März 1975. Danach ist für jedes innerhalb der Zentralverwaltung automatisiert geführte Register, das personenbezogene Daten enthält, eine besondere Satzung zu erlassen, die bestimmte Regelungen zum Schutz der gespeicherten personenbezogenen Daten enthalten muß. Alle Satzungen werden gesammelt und sind einsehbar. Die Rechte des Betroffenen auf Auskunft, Berichtigung und Löschung sind gewährleistet.

5.2.7.4 Großbritannien

Der Bericht einer unabhängigen Studienkommission ist am 5. Dezember 1978 veröffentlicht worden. Die wesentlichen Empfehlungen der Kommission lassen sich etwa wie folgt zusammenfassen:

Eine unabhängige Datenschutzbehörde (Data Protection Authority, DPA) soll eingesetzt werden, die aus einem Board von acht Mitgliedern und einem Stab von etwa 40 Personen bestehen soll. Die Aufgaben und Pflichten der DPA seien festzulegen. Ihr sei die Befugnis zu verleihen, Richtlinien (Codes of Practice) für bestimmte Bereiche, in denen besonders sensible Daten verarbeitet werden, zu erlassen. Diese Regelungen sollten vor ihrer Verabschiedung mit allen Beteiligten eingehend beraten werden. Jede Form der Datenverarbeitung, auf die derartige Richtlinien anzuwenden seien, müsse der Registrierung unterliegen. Die DPA solle allerdings die Möglichkeit erhalten, in besonderen Fällen Ausnahmen von der Registrierungspflicht zuzulassen. Dies gelte jedoch nicht für öffentliche Register. Alle auf diese Weise registrierten Formen der Datenverarbeitung müßten durch die DPA überwacht werden. Verstöße gegen die Richtlinien seien als Straftatbestand zu ahnden. Die Aufklärung solcher Verstöße müßte der DPA, nicht der Polizei übertragen werden. Die DPA solle ferner das Recht haben, auf Beschwerden Betroffener hin kontrollierend tätig zu werden. In Einzelfällen, in denen die Befolgung der Richtlinien eine unangemessene Härte darstellen oder unverhältnismäßige Kosten verursachen würde, solle der DPA die Befugnis gegeben werden, Ausnahmen zuzulassen. Die für die einzelnen Bereiche zu erlassenden Richtlinien müßten sicherstellen, daß

— der Betroffene erfahren könne, welche Daten über ihn verarbeitet werden, warum, wozu und wie lange sie benötigt werden;

— die Daten nur in dem Umfang und zu dem Zweck verwendet werden, zu dem sie erhoben worden sind; es sei denn, daß für eine anderweitige Nutzung eine ausdrückliche Ermächtigung vorliege;

— die Daten richtig, vollständig, relevant, auf dem neuesten Stand — gemessen an ihrer Zweckbestimmung — seien;

— der Betroffene feststellen könne, ob die Daten in Übereinstimmung mit der jeweiligen Richtlinie verarbeitet würden;

— die Kosten, die auf diese Weise entstünden, möglichst gering gehalten würden.

Um die Unabhängigkeit der DPA zu gewährleisten, sei es geboten, die Mitglieder des Board durch die Krone ernennen zu lassen. Der Mitarbeiterstab dürfe nicht aus Angehörigen des öffentlichen Dienstes bestehen. Die laufende Finanzierung müsse ausschließlich durch die Registrierungsgebühren erfolgen. Keine Regierungsstelle solle das Recht haben, die Richtlinien zu ändern oder zu ergänzen.

Für bestimmte Bereiche sollen nach den Vorstellungen der Kommission besondere Regelungen getroffen werden. Es sind dies die Bereiche: Verbrechensbekämpfung, nationale Sicherheit, Gesundheit, Sozialwesen, Personalwesen, Erziehungsbereich, Statistik und Forschung.

Die britische Regierung wird voraussichtlich nicht sogleich über die Vorschläge der Kommission entscheiden, sondern erst die Ergebnisse der nunmehr einsetzenden öffentlichen Diskussion abwarten.

5.2.7.5 Italien

In Italien hat eine von der Regierung gebildete Expertenkommission ihren Bericht vorgelegt. Sie schlägt vor, ein umfassendes Datenschutzgesetz zu erlassen. Wann der Bericht durch die Regierung veröffentlicht werden wird, ist noch offen.

5.2.7.6 Schweiz

In der Schweiz gibt es für den Kanton Genf ein Datenschutzgesetz, das am 1. März 1977 in Kraft getreten ist (Loi sur la protection des informations traitées automatiquement par ordinateur vom 24. Juni 1976, Offizielle Gesetzessammlung B. 4.12). In anderen Kantonen werden Entwürfe vorbereitet. Auf Bundesebene hat eine Expertenkommission 1974 einen Gesetzentwurf für eine Neugestaltung des Persönlichkeitsrechts vorgelegt. 1977 wurde durch eine parlamentarische Einzelinitiative die Forderung nach einer bundeseigenen Regelung „zum verstärkten Schutz der Persönlichkeit, der persönlichen Entfaltung und beruflichen Betätigung und der Privatsphäre jedes Menschen" (vgl. Übersicht über die Verhandlungen der Bundesversammlung I/II/1977, S. 10) erhoben. Gegenwärtig wird im Justizministerium ein Gesetzentwurf für den Datenschutz in der Bundesverwaltung vorbereitet. Darüber hinaus ist eine Kommission beauftragt worden, für den Datenschutz im privaten Bereich Vorschläge zu entwickeln.

5.2.7.7 Spanien/Portugal

In Spanien wird der Entwurf eines Datenschutzgesetzes vorbereitet. Er soll sich auf den Schutz automatisiert verarbeiteter Daten beschränken. Am 6. De-

zember 1978 ist die spanische Verfassung durch ein Referendum angenommen worden. Sie enthält in Artikel 18 Abs. 4 eine Datenschutzgarantie.

Ebenso hat nach Artikel 33 der portugiesischen Verfassung, die am 2. April 1976 verkündet und am 10. April 1976 im Diário da Republica (I. Série Nr. 86) veröffentlicht worden ist, jedermann ein Recht auf Schutz der Privatsphäre in seinem persönlichen Bereich und seinem Familienleben (nach einer offiziellen englischen Übersetzung: Everyone shall have the right to his personal identity, to his good name and reputation and to privacy in his personal and family life). Die aus diesem Grundrecht erwachsenden Rechte und Pflichten sind in Artikel 35 der Verfassung aufgeführt (Text bei 6.1).

5.2.8 Datenschutz in außereuropäischen Ländern

5.2.8.1 USA

Die nach Maßgabe des Datenschutzgesetzes 1974 gebildete Studienkommission hat ihren Bericht am 12. Juli 1977 abgeliefert. Er enthält etwa 165 eingehend begründete Empfehlungen. Der Bericht ist in der amerikanischen Öffentlichkeit und von der Regierung sehr positiv aufgenommen worden. Die zuständigen Regierungsstellen haben inzwischen ihre Stellungnahmen abgegeben. Dem Präsidenten ist eine Zusammenfassung dieser Äußerungen mit Vorschlägen für die weitere Gesetzgebungsarbeit vorgelegt worden. Nach der Entscheidung des Präsidenten sind Gesetzgebungsinitiativen auf der Basis der Empfehlungen der Kommission zu erwarten.

Ein erstes Ergebnis dieses Berichts ist der jüngst verabschiedete Financial Institutions Regulatory Act, dessen Titel XI die Überschrift trägt: „Right to Financial Privacy" (HR 14279—57). Mit diesem Gesetz wird der Zugriff öffentlicher Stellen auf die bei einer Bank über den Bankkunden geführten Unterlagen eingeschränkt. Das Gesetz bestimmt, daß

— jede Bundesbehörde, die Einsicht in bei einer Bank gespeicherte Daten eines Bankkunden verlangt, dies schriftlich erklären muß,

— der Betroffene zuvor von der öffentlichen Stelle unterrichtet werden muß,

— dieser die Rechtmäßigkeit des Ersuchens vor Gericht bestreiten kann,

— die Übermittlung der so erlangten Daten an andere Stellen der Bundesverwaltung nur zulässig ist, wenn auch der Empfänger sie selbst erheben dürfte. Der Empfänger muß bestätigen, daß dies der Fall ist. Die absendende Behörde muß den Betroffenen von der Übermittlung unterrichten.

Das Gesetz wird Anfang 1979 in Kraft treten.

Darüber hinaus ist in den einzelnen Bundesstaaten der USA eine lebhafte gesetzgeberische Aktivität im Bereich des Datenschutzes zu beobachten. Fast alle Staaten haben inzwischen für den Bereich ihrer öffentlichen Verwaltung ein dem Privacy Act 1974 entsprechendes Gesetz erlassen. In etwa 22 Staaten gibt es Gesetze, die den Datenschutz im Bereich des Bankwesens zum Gegenstand haben.

In den vergangenen zwei Jahren sind in 36 Staaten insgesamt 350 Gesetzentwürfe eingebracht worden, die das Zugangsrecht zu öffentlichen Unterlagen und den Datenschutz in verschiedenen Bereichen zum Gegenstand haben.

5.2.8.2 Kanada

Kanada hat den Datenschutz nicht in einem eigens dafür erlassenen Gesetz geregelt, sondern ein umfassenderes Gesetz, das kanadische Menschenrechtsgesetz erlassen, das am 14. Juli 1977 verabschiedet worden und am 1. März 1978 in Kraft getreten ist (Canada Gazette Part III, Vol. 2, Nr. 7, Chapter 33). Dieses Gesetz dient einem doppelten Zweck:

— einmal soll es sicherstellen, daß jedermann seine Persönlichkeit im Rahmen der Rechtsordnung entfalten kann, ohne wegen seiner Rasse, Nationalität, seines Alters, Geschlechts, Familienstandes, seiner religiösen Überzeugung oder aus anderen Gründen darin beeinträchtigt zu werden,

— ferner soll es die Privatsphäre des einzelnen schützen sowie sein Recht auf Zugang zu ihn betreffenden Informationen gewährleisten.

Das Gesetz verbietet im einzelnen diskriminierende Praktiken und gibt jedermann das Recht, sich an die Menschenrechts-Kommission zu wenden. Diese kann den Beschwerden nachgehen und Abhilfe nach bestimmten Verfahrensregeln zu erreichen suchen.

Sie kann auch ein sog. Menschenrechts-Tribunal bilden, dem gerichtsähnliche Befugnisse übertragen werden. Gegen die Entscheidung dieses Gremiums kann ein Überprüfungstribunal angerufen werden.

Der Teil des Gesetzes, der den Schutz der Privatsphäre zum Gegenstand hat, bezieht sich auf personenbezogene Daten, die von staatlichen Stellen des Bundes in Informationssystemen verarbeitet werden. Über jedes dieser Informationssysteme sind alljährlich bestimmte Angaben zu veröffentlichen. Aufgrund dieser Angaben kann der Bürger von seinem Auskunftsrecht gezielt Gebrauch machen. Die Auskunft ist gebührenfrei. Sind personenbezogene Daten für einen bestimmten administrativen Zweck erhoben worden und sollen sie auch für andere Zwecke verwendet werden, ist der Betroffene darüber zu unterrichten. Erhebt er nicht binnen einer festgesetzten Frist Einspruch, gilt sein Schweigen als Zustimmung. Die Ausnahmen von der Veröffentlichungs- und der Auskunftspflicht sind im Gesetz detailliert aufgeführt. Sie gehen teilweise über die im Bundesdatenschutzgesetz aufgeführten Ausnahmen hinaus; so kann zum Beispiel die Verpflichtung zur Auskunftserteilung im Hinblick auf bestimmte Informationssysteme generell ausgeschlossen werden, wenn der Nutzen durch die Auskunftserteilung in keinem Verhältnis zu den dadurch entstehenden Kosten stünde. Jeder Minister ist verpflichtet, die Nutzung der in seinen Zuständigkeitsbereich fallenden Informationssysteme mit dem Ziel zu koordinieren, die Erhebung von Daten auf das unbedingt notwendige Maß zu beschränken und die Nutzungsmöglichkeiten eindeutig festzu-

legen. Jede beabsichtigte Nutzungsänderung bedarf der Zustimmung des zuständigen Fachministers.

Für die Kontrolle des Datenschutzes ernennt der Justizminister auf Vorschlag des Vorsitzenden der Menschenrechtskommission ein Mitglied dieser Kommission zum Datenschutzbeauftragten. Dieser hat das Recht und die Pflicht, Beschwerden Betroffener nachzugehen. Er kann zu diesem Zweck Diensträume betreten und die ihm angemessen erscheinenden Untersuchungen durchführen. Führt nach Auffassung des Datenschutzbeauftragten die Untersuchung nicht zu einem befriedigenden Ergebnis, kann er sich an den zuständigen Minister wenden und ihn unter Fristsetzung um eine Stellungnahme ersuchen. Hält er auch diese Stellungnahme für unbefriedigend oder unzureichend, kann er dies dem Betroffenen mitteilen. Seine kritischen Äußerungen kann er auch in seinen Jahresbericht aufnehmen, den er dem Justizminister vorlegt, der ihn seinerseits an das Parlament weiterleitet.

5.2.8.3 Neuseeland

Im Mai 1978 besuchte mich der neuseeländische Ombudsman, Herr Laking, und berichtete über seine Erfahrungen im Hinblick auf die Kontrolle des Datenschutzes nach Maßgabe des neuseeländischen Datenschutzgesetzes. Dieses Gesetz ist am 9. September 1976 erlassen worden. Es bezieht sich auf die automatisierte Datenverarbeitung in der Wanganui Computer-Zentrale und wird danach als „Wanganui Computer Centre Act 1976" bezeichnet. In diesem zentralen Informationssystem werden Daten aus dem Bereich der Polizei, Justiz und des Verkehrswesens gespeichert (z. B. Dateien über Fingerabdrücke, Waffen, als gestohlen gemeldete Sachen oder Fahrzeuge, vermißte oder gesuchte Personen, Strafregister, Register über einsitzende Strafgefangene, Führerscheinregister, Register über Fahrzeugnummern, statistische Informationen). In einem Anhang zu dem Gesetz sind die zugelassenen Dateien, die Art der darin zu speichernden Daten und die Zugriffsberechtigungen im einzelnen aufgeführt. Sollen weitere Dateien geführt oder die bestehenden ergänzt werden, so ist dies nur in einem besonders vorgeschriebenen Verfahren möglich.

Das Gesetz dient einem doppelten Zweck: einmal soll es sicherstellen, daß die angeschlossenen Stellen der Justiz, Polizei und des Verkehrswesens ihre Aufgaben effektiv erfüllen können. Darüber hinaus soll es gewährleisten, daß das System nicht zu unzulässigen Einbrüchen in die Privatsphäre mißbraucht wird. Zu diesem Zweck wird ein Datenschutzbeauftragter bestellt, dessen Aufgaben im wesentlichen darin bestehen,

— Anträge Betroffener auf Auskunft entgegenzunehmen und zu bearbeiten,

— Beschwerden einzelner nachzugehen,

— sich zur Anzahl und Aufteilung zusätzlicher Terminals zu äußern und

— aus eigener Initiative ihm geboten erscheinende Kontrollen durchzuführen.

Das Verfahren der Auskunftserteilung unter Beteiligung des Datenschutzbeauftragten konnte eingeführt werden, weil nur aus dem einen Wanganui-Informationssystem Auskünfte zu erteilen sind. Anfängliche Schwierigkeiten bei der Auskunftserteilung (Anpassung des Systems, Identifizierung der in Betracht kommenden Daten, Übermittlung an den richtigen Adressaten, Erläuterung der Ausdrucke) sind inzwischen behoben worden. In einigen Fällen hat die Polizei im Einvernehmen mit dem Datenschutzbeauftragten nur über einen Teil der Daten Auskunft erteilt. Hinsichtlich des Restes standen Sicherheitsbedenken entgegen. In anderen Fällen hat sich der Datenschutzbeauftragte über das Votum der Polizei, die Auskunft nicht zu erteilen, hinweggesetzt und dem Betroffenen die erbetenen Unterlagen voll verfügbar gemacht.

Der ersten Datenschutzbeauftragte hat dieses Amt in Personalunion mit dem Amt des allgemeinen Ombudsmannes ausgeübt. Dies erwies sich wegen der Unterschiedlichkeit der Aufgaben als unzweckmäßig, so daß er zum 1. April 1978 seinen Rücktritt als Datenschutzbeauftragter erklärt hat. Ein Nachfolger ist inzwischen bestellt worden.

5.2.8.4 Australien

In Australien ist die Datenschutzgesetzgebung weitgehend Sache der Länder. Im Bundesstaat Neusüdwales gibt es ein Datenschutzgesetz. Dort ist auch ein Datenschutzbeauftragter eingesetzt worden.

Dem australischen Parlament liegt ferner ein Entwurf vor, der dem Bürger Zugang zu Akten der Bundesverwaltung geben soll. Er entspricht dem schwedischen Muster.

5.3 Probleme des grenzüberschreitenden Datenverkehrs

Die sich entwickelnde nationale Datenschutzgesetzgebung wird sicher dazu beitragen, daß der grenzüberschreitende Datentransport künftig erleichtert werden wird. Es bleiben jedoch Probleme: Einmal deckt die nationale Gesetzgebung, soweit sie vorhanden ist, nicht alle in Betracht kommenden Bereiche ab. Ferner ist nicht damit zu rechnen, daß alle Länder eigene Datenschutzgesetze erlassen werden. Schließlich müssen dem betroffenen Bürger, dessen Daten ins Ausland übermittelt oder dort verarbeitet werden sollen, Verfahren verfügbar gemacht werden, durch die er seine Rechte wahrnehmen kann.

5.3.1 Internationales Datenschutz-Übereinkommen

Die Notwendigkeit internationaler Vereinbarungen zur Lösung der im Zusammenhang mit dem grenzüberschreitenden Datentransport auftretenden Probleme wurde schon frühzeitig erkannt. Der Organisation für wirtschaftliche Entwicklung und Zusammenarbeit (OECD) gebührt das Verdienst, erstmals auf die Probleme hingewiesen und entsprechende Initiativen eingeleitet zu haben. Im September 1977 veranstaltete sie in Wien ein internationales Sympo-

sium, das den bereits angelaufenen Bemühungen um die Vorbereitung einer internationalen Konvention zusätzliche Impulse gab. Gegenwärtig befaßt sich eine Expertengruppe aus Vertretern der Mitgliedstaaten der OECD mit dem Problem. Das Ergebnis dieser Beratungen soll die Verabschiedung einer OECD-Empfehlung sein.

Innerhalb der Europäischen Gemeinschaften sind die Anstöße für Datenschutzinitiativen der Kommission vom Europäischen Parlament und von der Bundesregierung ausgegangen. Auf deren Betreiben setzte die Kommission 1976 eine Expertengruppe ein, die die rechtlichen Möglichkeiten einer Lösung dieses Problems im Bereich der Europäischen Gemeinschaften prüft (vgl. dazu näher Ordemann, Grenzüberschreitender Datentransport — Internationales Datenschutzübereinkommen, ÖVD 6/77, 3 ff.).

Im Europarat sind die Vorarbeiten für den Entwurf einer Datenschutz-Konvention am weitesten gediehen. Aufbauend auf Artikel 8 der Menschenrechtskonvention hat der Europarat bereits in den Jahren 1973/74 zwei Empfehlungen verabschiedet, die Grundsätze für die Ausgestaltung des Datenschutzes im öffentlichen und privaten Bereich enthalten. Auf dieser Basis wird z. Z. der Entwurf einer Datenschutz-Konvention erörtert. Er enthält in einem ersten Teil einen Katalog grundlegender Datenschutzprinzipien, die von den Unterzeichnerstaaten in ihrer nationalen Gesetzgebung verwirklicht werden sollen. Dazu gehören z. B.:

— Personenbezogene Daten sollen nur in angemessener und gesetzmäßiger Weise erhoben und an Dritte übermittelt werden,

— sie sind nach den Grundsätzen der Zweckbestimmung zu verarbeiten,

— sie sind auf dem neuesten Stand zu halten, ggf. zu berichtigen und zu löschen, wenn sie nicht länger benötigt werden,

— für besonders sensible Daten (z. B. über religiöse oder politische Anschauungen, rassische Zugehörigkeit, Gesundheit oder Vorstrafen) sollen verschärfte Vorschriften erlassen werden,

— jedermann soll einen Auskunftsanspruch haben,

— jedermann sollen Rechtsbehelfe zur Verfügung stehen, wenn eine speichernde Stelle sich weigert, den Rechten der Betroffenen zu entsprechen,

— die Daten müssen angemessen gesichert werden.

In einem zweiten Teil enthält der Entwurf Verfahrensregelungen zur Kooperation der Mitgliedstaaten untereinander. In welcher Form diese Kooperation letztlich verwirklicht werden wird, ist noch offen. Die Meinungsbildung innerhalb der beteiligten Regierungen ist insoweit noch nicht abgeschlossen.

5.3.2 Bedeutung der internationalen Zusammenarbeit

Der Entwurf der geplanten Europarats-Konvention ist ein erster Schritt in die richtige Richtung. Ob allerdings die mit ihr angestrebten Ziele voll zu verwirklichen sein werden, erscheint noch nicht gesichert. Dies gilt namentlich für den ersten Teil des Entwurfs, der dem Zweck dient, die nationale Gesetzgebung insoweit zu harmonisieren, daß sie den im Entwurf aufgeführten Grundsätzen entspricht. Sicher wäre es zu wünschen, daß dies gelingt. Angesichts der voneinander abweichenden Rechtstraditionen in den einzelnen Mitgliedstaaten einerseits, des unterschiedlichen Entwicklungsstandes der automatisierten Datenverarbeitung andererseits wird dies jedoch eine sehr schwierige Aufgabe sein. Hinzu kommt, daß die bereits vorhandenen nationalen Datenschutzgesetze den Grundsätzen möglicherweise in Einzelheiten nicht voll entsprechen und verständlicherweise wenig Neigung besteht, so junge Gesetze zu novellieren, ehe Erfahrungen mit dem Vollzug im eigenen Land vorliegen. Es ist nicht auszuschließen, daß der in dem Grundsätzekatalog erreichbare gemeinsame Nenner so niedrig angesetzt werden wird, daß ein völliger Verzicht vorzuziehen wäre. Dies wäre dann der Fall, wenn abzusehen ist, daß künftige Gesetze sich an einem derartigen Katalog orientieren würden. Schon jetzt sind die Grundsätze in ihrer relativ allgemeinen Form weitgehend Kompromißformeln und nur noch von beschränkter Aussagekraft (ebenso Simitis, Grenzüberschreitender Datenaustausch — Notwendige Vorbemerkungen zu einer dringend erforderlichen Regelung, in: Konflikt und Ordnung, Festschrift für Murad Ferid, München 1978, S. 356 [373]). Es wäre zu wünschen, daß die Konvention in ihrer endgültigen Form erweist, daß derartige Befürchtungen unbegründet waren.

Angesichts dieser nicht völlig auszuschließenden Möglichkeiten gewinnt der 2. Teil der Konvention an Bedeutung.

Die Verfahren der Zusammenarbeit sollten so gestaltet werden, daß sie auch dann funktionieren, wenn sich das Datenschutzrecht in den Mitgliedstaaten unterschiedlich entwickeln sollte. Dann wird es möglich sein, dem betroffenen Bürger in Einzelfällen zu helfen und den grenzüberschreitenden Datentransport so zu lenken, daß dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Die nach dem Bundesdatenschutzgesetz eingerichteten Aufsichtsbehörden haben bisher nicht das Recht, auf den grenzüberschreitenden Datentransport in der Weise Einfluß zu nehmen, daß sie beabsichtigte Übermittlungen zu genehmigen hätten. Die Zusammenarbeit mit den Aufsichtsbehörden anderer Staaten kann aber dazu beitragen, Fälle rechtswidriger Datenübermittlungen festzustellen. Auf der Grundlage der so gewonnenen Erkenntnisse wäre es denkbar, in Einzelfällen die Einleitung von Strafverfahren zu veranlassen. Notfalls wird auch eine Änderung des BDSG ins Auge zu fassen sein. Für Überlegungen in dieser Richtung bedarf es jedoch weiterer Erfahrungen. Die von mir aufgenommenen Kontakte erweisen sich dabei als eine wertvolle Basis. Ich beabsichtige, sie im kommenden Jahr auszubauen, um sodann konkrete Vorschläge unterbreiten zu können.

6 Ausblick

6.1 Grundrecht auf Datenschutz

Das Land Nordrhein-Westfalen hat vor kurzem ein Grundrecht auf Datenschutz in seine Verfassung aufgenommen. Schon vorher hatten Österreich und Portugal Datenschutz-Grundrechte verfassungsmäßig festgeschrieben.*) In Kanada sind die Datenschutzbestimmungen Bestandteil des Human Rights Act. Vorschläge zur Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz sind von verschiedener Seite gemacht worden.

Eine solche Erweiterung des Grundrechtskataloges wäre als starke Hervorhebung und Bekräftigung des Datenschutzes zu begrüßen. Sie würde für jedermann deutlich machen, daß es sich beim Datenschutz nicht nur um formale, technische Regeln über die Organisation von Verwaltungsvorgängen handelt, sondern daß wesentliche Rechte des Bürgers geschützt werden müssen. Derartige Verfassungsbestimmungen sichern bestehende und künftig hinzukommende Datenschutzvorschriften gegen spätere Wiederaufhebung durch den Gesetzgeber. Sie können als Auslegungsrichtlinie für Verwaltung und Gerichte zusätzliche Wirkungen entfalten und auch den Gesetzgeber bei der Gestaltung neuer Vorschriften daran hindern, die schutzwürdigen Belange des Bürgers hinter Rationalisierungs- und Vereinfachungsbestrebungen zurücktreten zu lassen (vgl. Artikel 1 Abs. 3 GG).

Durch die Aufnahme in die Verfassung würden schließlich die Beschränkungen des Anwendungsbereiches relativiert, die das BDSG (aus Gründen, die bei seiner Schaffung wohl zwingend waren) enthält (vgl. oben 4.1).

Allerdings ist gegenwärtig nicht zu befürchten, daß Bundes- oder Landesparlamente in den Bemühungen um den Datenschutz hinter den erreichten Stand der Gesetzgebung zurückfallen oder gar Datenschutzgesetze wieder aufheben. Manche scheinen auch übertriebene Erwartungen in die verfassungsmäßige Festschreibung des Datenschutzes zu setzen; die Rechtsposition des einzelnen kann durch eine solche „Rangerhöhung" des Datenschutzes nur graduell und im wesentlichen wohl vor allem prozessual verbessert werden: die Zulässigkeit einer entsprechenden Verfassungsbeschwerde kann dann mit größerer Überzeugungskraft begründet werden. Der Datenschutz ist schon jetzt verfassungsrechtlich insofern abgestützt, als die Grundrechtsartikel 1 und 2 über den Schutz der Menschenwürde und die freie Entfaltung der Persönlichkeit grundsätzlich auch den Schutz des Bürgers vor dem Fehlgebrauch seiner personenbezogenen Daten gewährleisten. Auch an-

---

*) Verfassung des Landes Nordrhein-Westfalen, Artikel 4 Abs. 2:

Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur auf Grund eines Gesetzes in überwiegendem Interesse der Allgemeinheit zulässig.

Österreichisches Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten, Artikel 1 (Verfassungsbestimmung):

Grundrecht auf Datenschutz

§ 1 (1) Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat.

(2) Beschränkungen des Rechtes nach Absatz 1 sind nur zur Wahrung berechtigter Interessen eines anderen oder auf Grund von Gesetzen zulässig, die aus den in Artikel 8 Abs. 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (BGBl. Nr. 210/1958) genannten Gründen notwendig sind. Auch im Falle solcher Beschränkungen muß der vertraulichen Behandlung personenbezogener Daten Vorrang gegeben werden.

(3) Jedermann hat, soweit Daten über ihn automationsunterstützt verarbeitet werden, nach Maßgabe gesetzlicher Bestimmungen das Recht auf Auskunft darüber, wer Daten über ihn ermittelt oder verarbeitet, woher die Daten stammen, welcher Art und welchen Inhaltes die Daten sind und wozu sie verwendet werden.

(4) Jedermann hat, soweit Daten über ihn automationsunterstützt verarbeitet werden, nach Maßgabe gesetzlicher Bestimmungen das Recht auf Richtigstellung unrichtiger und das Recht auf Löschung unzulässigerweise ermittelter oder verarbeiteter Daten.

(5) Beschränkungen der Rechte nach Absatz 3 und 4 sind nur unter den in Absatz 2 genannten Voraussetzungen zulässig.

(6) Soweit Rechtsträger in Formen des Privatrechts tätig sind, ist das Grundrecht auf Datenschutz im ordentlichen Rechtsweg geltend zu machen.

Verfassung der Republik Portugal, Artikel 35 (Offizielle Übersetzung ins Englische):

1. All citizens shall have the right to information on the contents of data banks concerning them and on the use for which it is intended. They shall be entitled to require the said contents to be corrected and brought up to date.
2. Data processing shall not be used for information concerning a person's political convictions, religious beliefs or private life except in the case of non-identifiable data for statistical purposes.
3. Citizens shall not be given all-purpose national identification numbers.

dere Verfassungsartikel (Artikel 4, 5, 6, 12 GG) können in Auseinandersetzungen um Offenlegung oder Zurückhaltung von Daten rechtliche Bedeutung erlangen.

Die weitere Diskussion um ein Grundrecht auf Datenschutz kann also ohne Zeitdruck geführt werden. Sie hat eine Reihe verfassungspolitischer und juristisch-praktischer Aspekte, die bisher noch wenig bearbeitet worden sind. So ist der Zusammenhang oder auch Gegensatz von Schutz des Persönlichkeitsrechts und anderen Rechten des Bürgers zu beachten, die bei der Sammlung und dem Austausch von Infoarmationen relevant werden können. Es ist zu bedenken, daß Datenschutz nicht nur Geheimhaltung, sondern im Verhältnis zwischen betroffenen Bürgern und Datenverarbeitern gerade Transparenz gebietet. In einem sehr weiten Sinn kann man Datenschutz sogar als System von Regeln für die Verständigung zwischen Menschen und den für sie arbeitenden Organisationen ansehen. Da der technische Wandel sich derzeit unerhört schnell vollzieht, ist überdies die Gefahr nicht zu leugnen, daß bei voreiliger Festschreibung von Rechtsnormen künftige Entwicklungen übersehen werden. Während dies bei der einfachen Gesetzgebung nicht zu vermeiden und auch unschädlich ist, kann es sich bei dem aus guten Gründen erschwerten Verfahren der Verfassungsänderung als nachteilig erweisen.

Ich werde an der weiteren verfassungsrechtlichen und -politischen Diskussion teilnehmen und bei geeigneter Gelegenheit auf das Thema zurückkommen.

6.2 Technologische Entwicklung und Datenschutz

ADV-Systeme in all ihren Komponenten — also Anlagen, Betriebssysteme und Anwenderprogramme — sind bisher fast nur unter Leistungsgesichtspunkten entwickelt worden. Im Vordergrund stand dabei das Interesse der Betreiber, die vielfältigen Möglichkeiten des Computers zur Nutzung von Informationen auszuschöpfen. Um den Schaden aus Datenverlusten abzuwehren, sind allerdings auch Verfahren der Sicherung gegen Datenverluste entwickelt und angewendet worden, und die Anwender haben im eigenen Interesse Maßnahmen gegen mißbräuchliche Verwendung ihrer Systeme ergriffen. Vorkehrungen, die darüber hinaus der Verantwortlichkeit des Informationsverarbeiters für die Belange der Betroffenen Rechnung tragen, waren jedoch weder gefragt noch wurden sie bis vor kurzem überhaupt angeboten. Hier besteht bis heute in der Entwicklung ein erhebliches Defizit. Die gegenwärtig verfügbaren Datensicherungskonzepte stellen häufig nur Notlösungen dar. Solche Notlösungen können von Anwendern großer Systeme nachträglich in ihre Systeme eingebaut werden, bleiben aber auch dort oft unzulänglich. Die Anwender kleiner und mittlerer Systeme sind so gut wie außerstande, nachträgliche Schutzanforderungen zu erfüllen, wenn sie ihre Systeme einschließlich der Programme als Fertigprodukte eingesetzt haben.

Systeme, die den Anforderungen des Persönlichkeitsschutzes genügen, verlangen erheblichen Entwicklungsaufwand. Neben die bisher dominierenden Konstruktionsziele der Schnelligkeit und Wirtschaftlichkeit muß als gleichwertig die Forderung nach eingebauter Selbstkontrolle treten. Dazu bedarf es möglicherweise ganz anderer Denkansätze als der bisher üblichen. Technologie-Politiker wie der Bundesminister für Forschung und Technologie vertreten ohnehin den Standpunkt, daß eine andere, „ganzheitliche Denkweise" geboten sei, wenn wir den „Fehler der ersten industriellen Revolution vermeiden" wollen, den Fehler nämlich, Technologien ohne Berücksichtigung ihrer Folgeprobleme für den einzelnen und die Gesellschaft zu entwickeln und einzusetzen. Fehler und falsche Weichenstellungen von heute wirken sich auf die Realisierungschancen des Persönlichkeitsschutzes in der Zukunft aus.

Die aufgezeigte Problematik erfährt noch eine wesentliche Verschärfung durch das Entstehen und die Ausbreitung von Computer-Netzen. Der Preisrückgang für Rechenanlagen erlaubt es, Datenverarbeitung auf die einzelnen Arbeitsplätze zu verteilen, wobei mehr Daten erfaßt, aber auch den Zentralen zugeleitet und miteinander verknüpft werden können. Parallel dazu werden die technischen Voraussetzungen geschaffen, daß Daten zwischen verschiedenen, voneinander unabhängigen Systemen über öffentlich zugängliche Vermittlungsnetze ausgetauscht werden.

Auf internationaler Ebene werden technische Konventionen und Normen z. B. über Schnittstellen und Leitungsprozeduren geschaffen, um den Datenverkehr zu standardisieren und damit zu erleichtern. Auch wegen der zusätzlich entstehenden Schwachstellen auf dem Übermittlungsweg und im Satellitenverkehr muß für wirksame Schutzmechanismen gesorgt werden. Ohne eine intensive internationale Zusammenarbeit wird die Durchsetzung des Datenschutzes in der Bundesrepublik Deutschland in Zukunft schwieriger werden, weil die Technologie-Orientierung bei der Entwicklung neuer Systeme den Belangen des Datenschutzes aus der Sicht unserer Rechtsordnung möglicherweise nicht genügend Rechnung trägt.

Zu den im großen und ganzen bekannten Problemen kommen völlig neuartige, die sich mit dem Stichwort „Kabelkommunikation" verbinden. Bei aller Ungewißheit darüber, was aus den in Angriff genommenen Pilotprojekten herauskommen wird, ist schon heute die Möglichkeit erkennbar, daß ein großes System sozialer Kontrolle und Überwachung entsteht, wenn die individuelle Nutzung des neuen Informationsangebots detailliert aufgezeichnet wird. Um diese Gefahr abzuwenden, muß der Schutz der Persönlichkeit Bestandteil der entstehenden Systeme werden. Es muß sichergestellt werden, daß die sich ergebenden technischen Möglichkeiten nicht dazu mißbraucht werden, gezielt oder als Nebenprodukt das Kommunikationsverhalten der Bürger zu registrieren. Velmehr sind die technischen Einrichtungen von vornherein so zu gestalten, daß entsprechende Überwachungen nicht möglich sind. Wo die Technik entgegen dieser Forderung riskante Nutzungen zu-

läßt, ist für eine wirkungsvolle Kontrolle vorzusorgen.

Es ist nicht meines Amtes, die auf den angesprochenen Gebieten erforderlichen Entwicklungen selbst durchzuführen oder auch nur einzuleiten. Ich kann auch nicht das gelegentlich geforderte „Gütezeichen" für datenschutzgerechte Systeme vergeben. Ich bin aber bereit, die Erfahrungen aus meiner Tätigkeit in alle Bemühungen einzubringen, die den Persönlichkeitsschutz zur Richtschnur der künftigen informationstechnischen Entwicklungen machen. Technologiepolitik, Wissenschaft und Industrie sind aufgerufen, die neuen Methoden der Informationsverarbeitung in den Rahmen unserer freiheitlichen Ordnung einzufügen.

Sachregister